

Department of Veterans Affairs

Veterans Crisis Line (VCL)

Installation Guide



Version 0.6

December 2014

Revision History

Date	Version	Description	Author
12/01/2014	0.6	Technical edit. Added figure captions and two new screens to section 6.	REDACTED
6/25/14	0.5	Updated content and formatting	REDACTED
6/12/14	0.4	Updated with current installation instructions	REDACTED
05/08/2014	0.3	Removed Other Considerations section, which included 2008 server references. Added pre-prod links to Section 3.1, General Installation Flow.	REDACTED
05/06/2014	0.2	Modified web installation content to meet AITC standards.	REDACTED
3/25/2014	0.2	Added Raj's SSRS content. Added AITC content to pre-installation section. Reviewed and incorporated comments from SQA.	REDACTED
02/18/2014	0.2	Add MDWS installation instructions	REDACTED
02/06/14	0.2	Added instructions on how to obtain VCL code base.	REDACTED
6/3/2013	0.1	Created template	REDACTED

Table of Contents

Introduction	9
1.1. Overview	9
1.2. Audience	9
1.3. Scope	9
1.4. Veterans Crisis Line	9
1.5. Using This Manual	9
1.6. How Much Do I Need to Install?	10
1.7. Related Documentation	10
2. Preinstallation	13
2.1. Preinstallation Steps	13
2.2. System Backup	17
2.3. Retrieving Files from Staging Areas	17
2.3.1. Database Staging Area	17
2.3.2. Application Staging Area	17
3. Installation Prerequisites	18
3.1. SSL Setup	20
3.2. General VCL Installation Flow	21
3.3. MDWS installation	42
3.4. System Requirements	44
4. Backout Plan	45
5. Post Installation Instructions	47
6. Installing and Configuring the SQL Server Reports Server (SSRS) Component	48
6.1. Audience	48
6.2. Pre-Requisites	48
6.3. Configuring the Reports Server (Includes SSL)	49
6.4. Defining the Reporting Web Project	54
6.5. Reporting Services SSL Configuration	62
6.6. Uploading Previously Developed “Sample Reports” to the Server	62
7. Patching the Production Environment with Updated Code	64
8. Troubleshooting	66
8.1. Rollback Instructions	66
9. FAQ	67

List of Figures

Figure 1: VCL Application Flow	21
Figure 2: VCL Installed Components	23
Figure 3: VCL Add Features Wizard.....	24
Figure 4: VCL Installing Web Services Enhancements 3.0 – select Runtime option.....	25
Figure 5: Installing Web Services Enhancements 3.0 – Click Finish to complete installation.....	26
Figure 6: Unpack VCL Code Archive	27
Figure 7: IIS Manager.....	28
Figure 8: VCL Site Breakout	29
Figure 9: VCL Site Breakout Expanded	30
Figure 10: SSL Settings	30
Figure 11: Application Pools	31
Figure 12: Edit Application Pool settings.....	32
Figure 13: CrisisCenter Properties.....	33
Figure 14: Permissions for CrisisCenter	34
Figure 15: Locations	34
Figure 16: Enter the Object Names to Select.....	35
Figure 17: Check Names.....	35
Figure 18: Default Permissions.....	36
Figure 19: IIS Manager, CrisisCenter Virtual directory	37
Figure 20: Edit Application	38
Figure 21: Connect As dialogue.....	38
Figure 22: Crisis Center Hotline Login.....	40
Figure 23: CrisisCenter Response.....	41
Figure 24: CrisisCenter Administrator.....	41
Figure 25: Unpack VCL Code Archive	46
Figure 26: Reporting Services Configuration Connection.....	49
Figure 27: Reporting Services Configuration Manager.....	50

Figure 28: Specify a Server Name	50
Figure 29: Report Server Status	51
Figure 30: SSL Certificate and SSL Port	51
Figure 31: SSL Certification Information	52
Figure 32: Add Report Manager URL	52
Figure 33: UpdatingSSL Certificates	53
Figure 34: Create a Datasource	54
Figure 35: VCL Datasource	55
Figure 36: Generate Model	56
Figure 37: VCL Model.....	57
Figure 38: System User.....	58
Figure 39: New Role Assignment.....	58
Figure 40: Edit Role Assignment.....	59
Figure 41: Security.....	59
Figure 42: Properties.....	60
Figure 43: Veterans Crisis Line – Custom Reports	61
Figure 44: Upload File	63
Figure 45: Change Order Request Email	65

Introduction

This Veterans Crisis Line (VCL) Installation Guide provides information for Information Resource Management (IRM) personnel to install and configure the components of the VCL application.

1.1. Overview

The Office of Mental Health Services (OMHS) is currently managing a web-based application (herein referred to as VCL) utilized by their confidential, free 24-hours hotline staff to make referrals to the appropriate field-based Suicide Prevention Coordinators (SPCs).

OMHS is requesting OIT to assist OMHS to enhance, deploy and support the existing Veterans Crisis Line application and hardware platform utilizing Information Technology (IT) best practices and procedures rather than maintaining the existing ad-hoc environment.

1.2. Audience

This document has been prepared for system administrators and database administrators who need to set up development, pre-production and/or production environments at the Austin Information Technology Center (AITC). It is presumed that readers of this document understand basic concepts of the VCL environments as well as any system specialties that might pertain to the installation of the VCL software.

1.3. Scope

This Installation Guide includes steps for installing the Pre-Prod environment. Assumptions for installation include the following:

- Pre-installation steps have been completed.
- 9957's have been submitted 30 days prior to need date for each environment
- All backups have been performed
- All files have been placed into the appropriate staging area
- Application server certificates have been installed.

1.4. Veterans Crisis Line

1.5. Using This Manual

This manual guides the reader through a very specific order for installing and configuring the various components of VCL.

1.6. How Much Do I Need to Install?

Depending on your purposes for installing VCL components, you may not need to install all of the components described in this Installation Guide. Please follow these guidelines for determining which components you should install:

This Guide also covers the install from a total “ground-up” perspective. This involves the following additional steps:

- Restoring the VCL database from a backup file.
- Obtaining and installing the VCL code.
- Installing the appropriate version of SQL Server Reporting Services.
- Installing the correct version and configuration of IIS.
- Installing the correct version of MDWS web service.

1.7. Related Documentation

Refer to the following documentation for additional information about VCL.

The documentation will be in the form of Adobe Acrobat files.

Documentation can also be found on the [VA Software Documentation Library](#).

File Name	Description
VCL Production Operations Manual (POM).PDF	Includes system and operational description for VCL, information about routine operations, and contingency planning.
VCL_Release Notes.PDF	Release notes on new features and functionality
VCL_User Guide.PDF	VCL User Guide
VCL_Installation Guide.PDF	Installation Guide for installation in various environments

This page intentionally left blank for double-sided printing.

2. Preinstallation

The following sections include steps required to setup the development environment.

2.1. Preinstallation Steps

The following preinstallation steps need to be completed for the development environment:

Group Account Creation

1. Verify/Create Security Groups for Report Viewer and Manager (9957 or ePAS).
This function is now complete for all environments
 - a. Create the Groups used for User Management Access based on the specific environment and functions.
 - b. Groups Created
 - i. Dev
 1. VCLREPORTMANAGER_DEV
 2. VCLREPORTVIEWER_DEV
 - ii. Preproduction
 1. VCLREPORTMANAGER_PPD
 2. VCLREPORTVIEWER_PPD
 - iii. Production
 1. VCLREPORTMANAGER
 2. VCLREPORTVIEWER

CHECK APPROPRIATE BOX		NAME OF FUNCTIONAL TASK CODES; PROFILES, WEB SERVERS; UNIX ACCOUNTS; DATABASE OR OTHER ACCESS	DEFINE LEVEL OF ACCESS REQUESTED OR CONCURRING SYSTEM MANAGER OF RECORD (SMR) DESIGNEE SIGNATURE AND TITLE (If required)
ADD	DELETE		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTMANAGER_DEV	Create Security Group for VCL Report Management
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTVIEWER_DEV	Create Security Group for VCL Report Management
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTMANAGER_PPD	Create Security Group for VCL Report Management - Preprod
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTVIEWER_PPD	Create Security Group for VCL Report Management - Preprod
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTMANAGER	Create Security Group for VCL Report Management - Production
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTVIEWER	Create Security Group for VCL Report Management - Production

2. Submit request to grant permissions to the Security Groups created:
This function is now complete for Development
 - a. Granting permissions to these groups allow individuals to be added to the Security Groups rather than making multiple changes on the servers. Permissions and titles are specific to the environment, including the actual names of the database. These must be completed after the databases have been created.
 - b. Permissions Created so far:

i. Development

1. VCLREPORTMANAGER_DEV

- a. On the database server VAAUSSQL1a: Read permission on DB: "NationalSuicideHotline_Test1" R/W on DB's: VCLReportServer and VCLReportServerTempDB
- b. On the VAAUCVCLAPP80 in SQL Server Reporting Service Grant the following roles: Browser, Report Builder

2. VCLREPORTVIEWER_DEV

- a. On the database server VAAUSSQL1a: Read permissions on DB's: VCLReportServerTempDB, VCLReportServer and "NationalSuicideHotline_Test1"
- b. On the VAAUCVCLAPP80 in SQL Server Reporting Service Grant the following roles: Browser

3. ACCESS REQUESTED			
CHECK APPROPRIATE BOX		NAME OF FUNCTIONAL TASK CODES; PROFILES, WEB SERVERS; UNIX ACCOUNTS; DATABASE OR OTHER ACCESS	DEFINE LEVEL OF ACCESS REQUESTED OR CONCURRING SYSTEM MANAGER OF RECORD (SMR) DESIGNEE SIGNATURE AND TITLE <i>(If required)</i>
ADD	DELETE		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Please create the SQL database account listed below for the VCL Dev System	ATTN: Windows SQL Admin
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptRODev	Grant read only access to DB NationalSuicideHotline_Test on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptRODev	Grant read only access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppDev	Grant read/write access to DB NationalSuicideHotline_Test on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppDev	Grant read/write access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A

3. Submit request to add users to appropriate security groups (9957 or ePAS):

This function is now complete for Development.

Note: Developers have requested and been individually granted elevated privileges in the development environment. Elevated privileges are restricted to EO AITC Administrators in other environments.

REDACTED

3. ACCESS REQUESTED			
CHECK APPROPRIATE BOX		NAME OF FUNCTIONAL TASK CODES; PROFILES, WEB SERVERS; UNIX ACCOUNTS; DATABASE OR OTHER ACCESS	DEFINE LEVEL OF ACCESS REQUESTED OR CONCURRING SYSTEM MANAGER OF RECORD (SMR) DESIGNEE SIGNATURE AND TITLE <i>(If required)</i>
ADD	DELETE		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTMANAGER_DEV	Add the users in the attached spreadsheet to this security group: VCLREPORTMANAGER_DEV
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VCLREPORTVIEWER_DEV	Add this user and the users in the attached spreadsheet to this security group: VCLREPORTVIEWER_DEV

Service Account Creation

1. Verify/Create Application Service Accounts (9957 or ePAS) – **This function is now complete for all environments**
 - a. Create the accounts used for the application to connect to the database based on the specific environment and functions.
 - b. Service Accounts Created
 - i. Dev
 1. VaAacVclAppDev - Development Application Service Account
 2. VaAacVclRptRODev - Development Reporting Service Account
 - ii. Preproduction
 1. VaAacVclAppPpd - PreProduction Application Service Account
 2. VaAacVclRptROPpd - PreProduction Reporting Service Account
 - iii. Production
 1. VaAacVclAppPrd - Production Application Service Account
 2. VaAacVclRptROPrd - Production Reporting Service Account

CHECK APPROPRIATE BOX		NAME OF FUNCTIONAL TASK CODES; PROFILES, WEB SERVERS; UNIX ACCOUNTS; DATABASE OR OTHER ACCESS	DEFINE LEVEL OF ACCESS REQUESTED OR CONCURRING SYSTEM MANAGER OF RECORD (SMR) DESIGNEE SIGNATURE AND TITLE <i>(If required)</i>
ADD	DELETE		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Create the following Service Accounts:	These accounts will be user by the Application and Reporting tools to access data
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppDev	Development Application Service Account
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppPpd	PreProduction Application Service Account
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppPrd	Production Application Service Account
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptRODev	Development Reporting Service Account
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptROPpd	PreProduction Reporting Service Account
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptROPrd	Production Reporting Service Account

2. Submit request to grant permissions to the Security Groups created: **This function is complete for Development**

- a. Granting permissions to these groups allow the application to connect to the database. Permissions and titles are specific to the environment, including the actual names of the database. These must be completed after the databases have been created.
- b. Permissions Created so far:
 - i. Dev
 1. VaAacVclAppDev
 - a. Grant read/write access to DB NationalSuicideHotline_Test on VAAUSSQL1A
 - b. Grant read/write access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A
 2. VaAacVclRptRODev
 - a. Grant read only access to DB NationalSuicideHotline_Test on VAAUSSQL1A
 - b. Grant read only access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A

3. ACCESS REQUESTED			
CHECK APPROPRIATE BOX		NAME OF FUNCTIONAL TASK CODES; PROFILES, WEB SERVERS; UNIX ACCOUNTS; DATABASE OR OTHER ACCESS	DEFINE LEVEL OF ACCESS REQUESTED OR CONCURRING SYSTEM MANAGER OF RECORD (SMR) DESIGNEE SIGNATURE AND TITLE <i>(If required)</i>
ADD	DELETE		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Please create the SQL database account listed below for the VCL Dev System	ATTN: Windows SQL Admin
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptRODev	Grant read only access to DB NationalSuicideHotline_Test on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclRptRODev	Grant read only access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppDev	Grant read/write access to DB NationalSuicideHotline_Test on VAAUSSQL1A
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VaAacVclAppDev	Grant read/write access to DB NationalSuicideHotline_Test1 on VAAUSSQL1A

2.2. System Backup

Austin Information Technology Center (AITC) system backup procedures include the following:

- Backing up the system
- VMWARE Consolidated BACKUP
- Request snapshot of entire server image. Snapshots are only completed upon request and are deleted after eight hours.
- Backup of the database

Note: Full backups are performed on the system every Friday. Differential backups are performed daily.

2.3. Retrieving Files from Staging Areas

2.3.1. Database Staging Area

The VCL Development team drops files for the Dev and PPD instance here: vaausvclapp80\vcl. Production Data Transfer will be handled according to protocols defined in a separate “Data Transfer Agreement.”

2.3.2. Application Staging Area

The VCL Development team drops files for the application server here: vaausvclapp80\vcl.

3. Installation Prerequisites

The following preinstallation requirements apply for users who are installing VCL:

- Windows server needs to be installed on to the target environment.
- The environment will vary based on utilization (PPD).
- Technical Manager / Configuration Manager has submitted all the firewall rules.
- Sufficient disk space is available on the application server as specified by AITC
- Database Administrator has approved 9957's to create application accounts and roles
- Microsoft Web Service Extension 3.5
- Microsoft .Net Framework 4.0, which can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=17718>.
- IIS 7
 - MDWS can be installed in a new virtual directory.
- MDWS installation reference, located at http://vaww.oed.portal.va.gov/projects/vet_crisis_line_enhancements/Library/User%20Documentation%20and%20National%20Release/mwvs2_0ig.doc.
- Windows Server 2008 with IIS 7.0.
 - Install Microsoft .NET 3.5.1
 - Install Static Content
- A shared SQL Server Database is to be utilized. Here are the desired version specifics:
 - Database Version 10.0.1600.22 (Note, this is the SQL Server 2008 Non-R2 version)
- The SQL Server Management Studio is will be installed on the PPD Servers. Here are the version specifics:

• Microsoft SQL Server Management Studio	10.0.1600.22 ((SQL_PreRelease).080709-1414)
• Microsoft Data Access Components (MDAC)	6.1.7601.17514 (win7sp1_rtm.101119-1850)
• Microsoft MSXML	2.6 3.0 4.0 5.0 6.0
• Microsoft Internet Explorer	9.10.9200.16750

• Microsoft .NET Framework	2.0.50727.5472
• Operating System	6.1.7601

- SQL Server Reporting Services (SSRS) is to be installed on an application server. In the PPD instances, this will be installed on the only Application Server. In PRD, this should be installed on a server selected based on load balancing needs. The SSRS version as well as the Business Intelligence Development Studio version details are listed below:

• Microsoft Visual Studio 2008	Version 9.0.30729.1 SP
• Microsoft .NET Framework	Version 3.5 SP1
• Installed Edition: IDE Standard	
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB945282)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB946040)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB946308)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB946344)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB946581)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB947173)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB947540)
• Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB947789)
• Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB2251487)
• Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU	(KB2669970)

- Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB972222)
- SQL Server Analysis Services
- Microsoft SQL Server Analysis Services Designer
- Version 10.50.4260.0
- SQL Server Integration Services
- Microsoft SQL Server Integration Services Designer
- Version 10.0.1600.22 ((SQL_PreRelease).080709-1414)
- SQL Server Reporting Services
- Microsoft SQL Server Reporting Services Designers
- Version 10.0.1600.22

3.1. SSL Setup

The VCL will provide PII information. To be complaint with government, VCL will encrypt all communication between client browser and server.

VCL has a total of three web sites. One requires a signed certificate. The SSL web site will have three sub-sites, which will be the three VCL web applications.

AITC will take responsibility for the SSL setup.

Dev

REDACTED

Pre-Prod

REDACTED

Prod

REDACTED

3.2. General VCL Installation Flow

The following flow diagram illustrates an overview of the basic information flow of the application. This installation does not include the Vista servers, only verifying the MDWS-Vista connection.

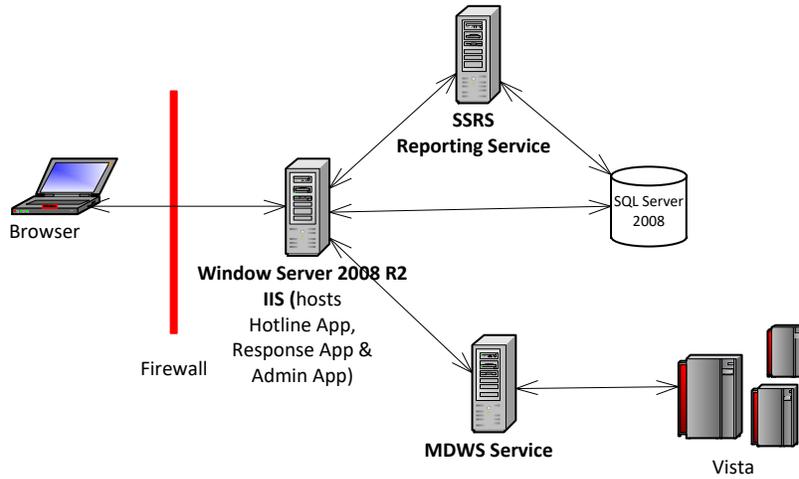
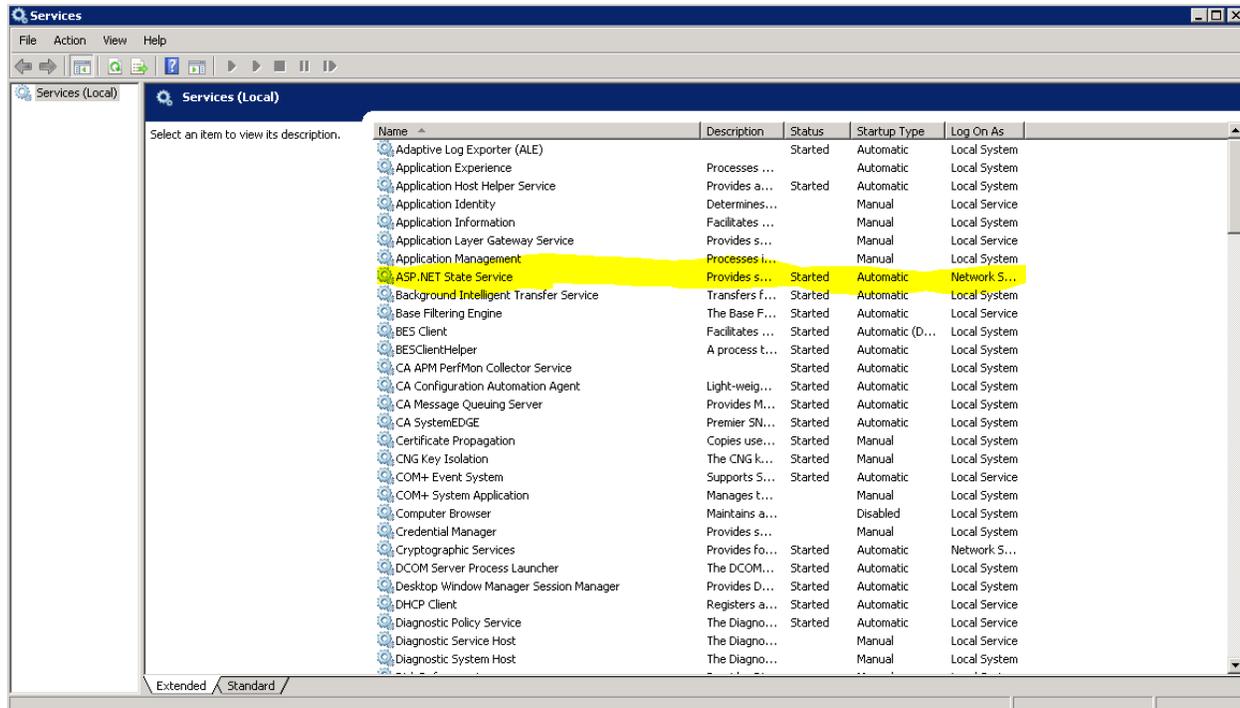


Figure 1: VCL Application Flow

IIS Installation Settings

1. Verify IIS is installed with default settings with the following exceptions:
 - a. Install Microsoft .NET 3.5.1
 - b. Install Static Content
 - c. Install Web Services Enhancements 3.0
 - d. Verify the ASP.NET Session State Service is set to a startup type of Automatic, and is running.



	Web Server	Installed
	Common HTTP Features	Installed
	Static Content	Installed
	Default Document	Installed
	Directory Browsing	Not installed
	HTTP Errors	Not installed
	HTTP Redirection	Not installed
	WebDAV Publishing	Not installed
	Application Development	Installed
	ASP.NET	Installed
	.NET Extensibility	Installed
	ASP	Not installed
	CGI	Not installed
	ISAPI Extensions	Installed
	ISAPI Filters	Installed
	Server Side Includes	Not installed
	Health and Diagnostics	Not installed
	HTTP Logging	Not installed
	Logging Tools	Not installed
	Request Monitor	Not installed
	Tracing	Not installed
	Custom Logging	Not installed
	ODBC Logging	Not installed
	Security	Installed
	Basic Authentication	Not installed
	Windows Authentication	Not installed
	Digest Authentication	Not installed
	Client Certificate Mapping Authentication	Not installed
	IIS Client Certificate Mapping Authentication	Not installed
	URL Authorization	Not installed
	Request Filtering	Installed
	IP and Domain Restrictions	Not installed
	Performance	Not installed
	Static Content Compression	Not installed
	Dynamic Content Compression	Not installed
	Management Tools	Installed
	IIS Management Console	Installed
	IIS Management Scripts and Tools	Not installed
	Management Service	Not installed
	IIS 6 Management Compatibility	Not installed
	IIS 6 Metabase Compatibility	Not installed
	IIS 6 WMI Compatibility	Not installed
	IIS 6 Scripting Tools	Not installed
	IIS 6 Management Console	Not installed

Figure 2: VCL Installed Components

IIS Installed Components

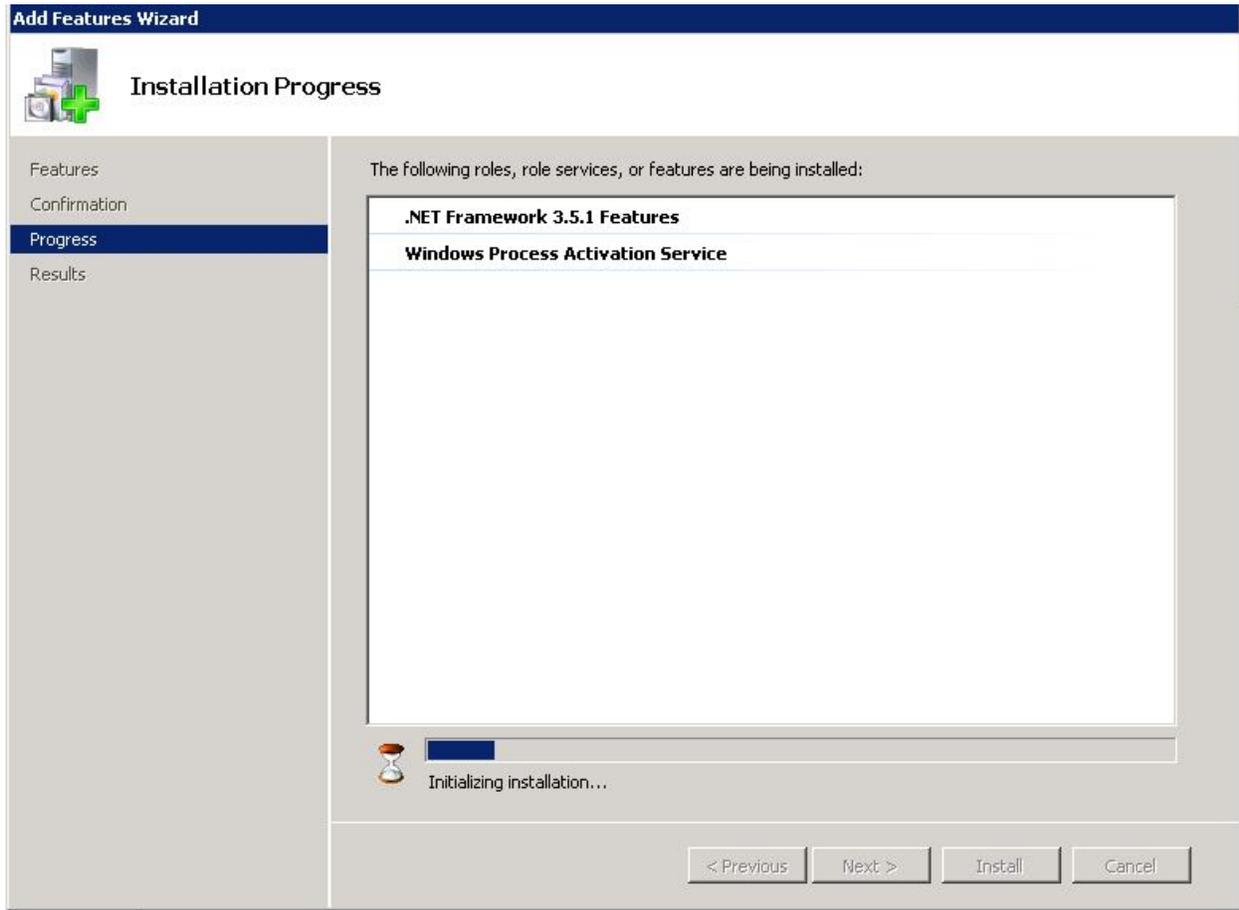


Figure 3: VCL Add Features Wizard

IIS Additional Components

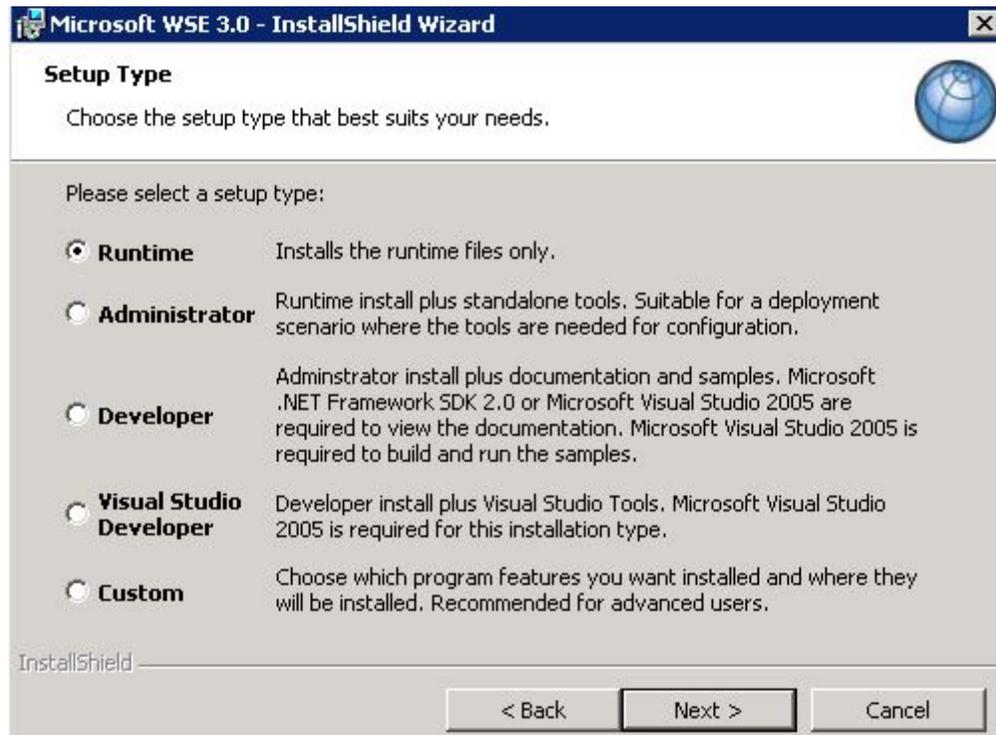


Figure 4: VCL Installing Web Services Enhancements 3.0 – select Runtime option



Figure 5: Installing Web Services Enhancements 3.0 – Click Finish to complete installation

Locate VCL Code

2. The VCL code will be uploaded onto the dev server in the location `vausvclapp80\vcl\vcl-####.zip`. It will be in an archive, with a naming convention that identifies the version, and when unpacked will have a directory structure similar to the following:

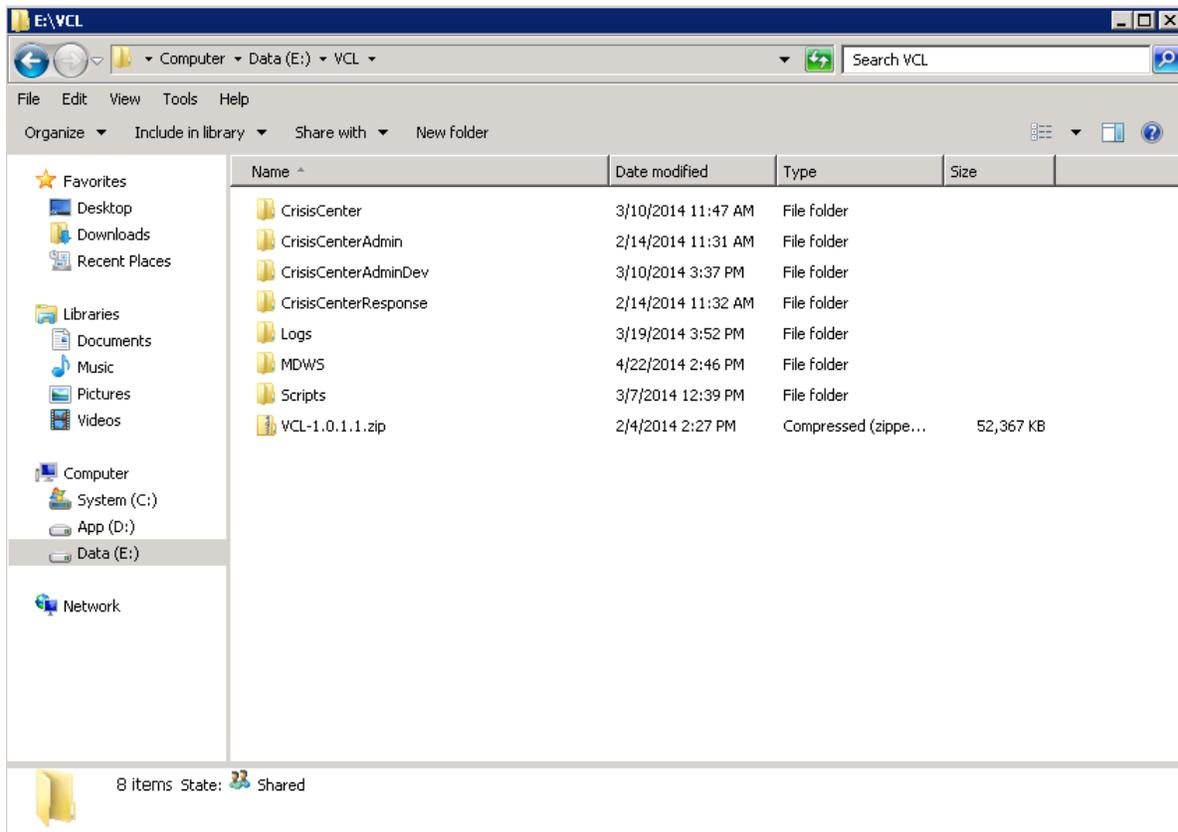


Figure 6: Unpack VCL Code Archive

Unpack the VCL code archive to E:\VCL. The folder structure should look similar to the following:

Create and set up VCL web sites

3. Open IIS Manager.

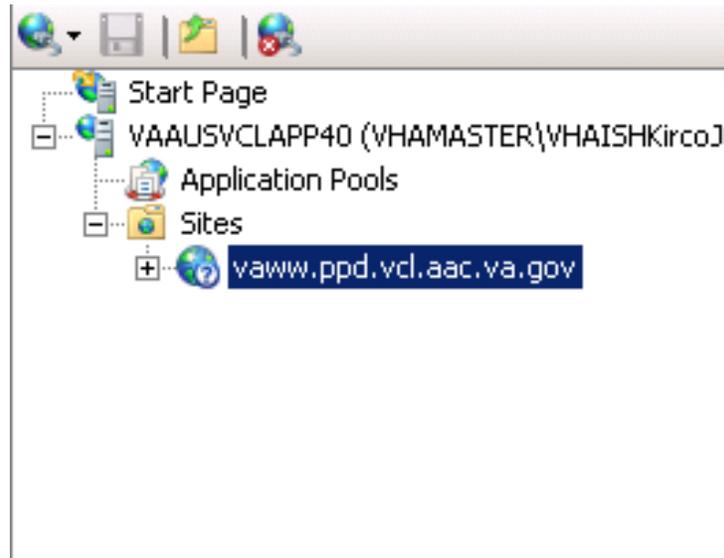


Figure 7: IIS Manager

4. In IIS Manager, go to IIS -> Authentication
5. Select "Anonymous Authentication" then select "Edit"
6. Under the "Edit Anonymous Authentication Credentials" window, make sure "Application Pool Identity" is selected.
7. Rename default site to server website name.
8. There are three applications to be created under the server website name. Right-click the server website name, and select "Add Application"

Please note that the creation of the web sites will also create the application pools, which is detailed in step b under the creation of each web application (steps 5, 6, and 7).

9. Fill in the following information for the CrisisCenter web application:
 - a. Site name: CrisisCenter
 - b. Application pool: CrisisCenter
 - c. Physical path: E:\VCL\CrisisCenter
10. Fill in the following information for the Response web application:
 - a. Site name: Response
 - b. Application pool: Response
 - c. Physical path: E:\VCL\CrisisCenterResponse

11. Fill in the following information for the Admin web application:
 - a. Site name: Admin
 - b. Application pool: Admin
 - c. Physical path: E:\VCL\CrisisCenterAdmin
12. IIS Manager should look similar to the following when you are done:

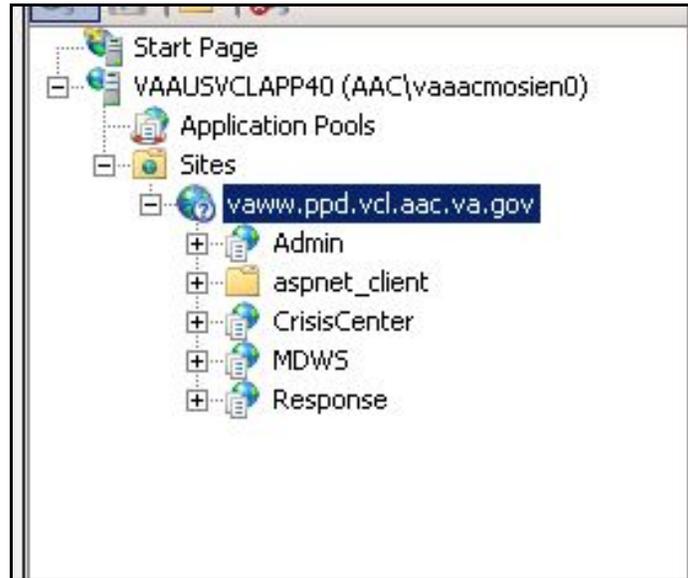


Figure 8: VCL Site Breakout

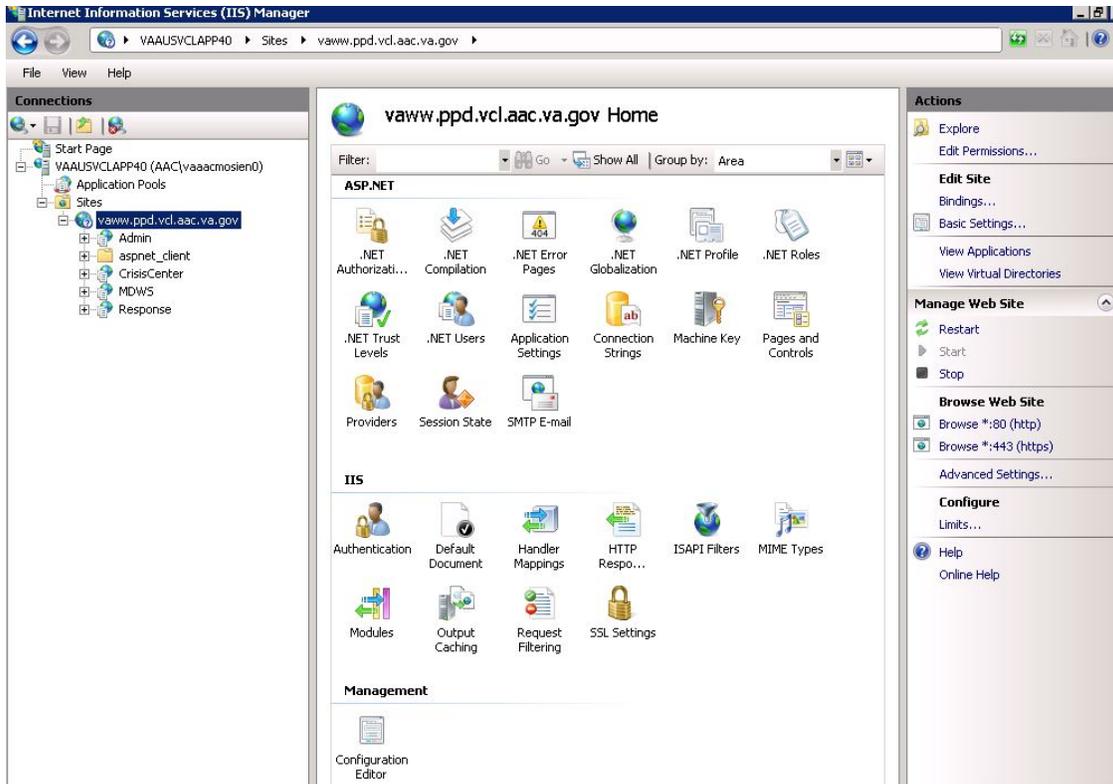


Figure 9: VCL Site Breakout Expanded

Require SSL

13. Add the HTTPS bindings to the website certificate using whatever process you have in place to accomplish this.
14. Select the newly created website, then double-click SSL Settings. Select Require SSL, and click Apply.



Figure 10: SSL Settings

Modify application pools

15. In IIS Manager, click Application Pools

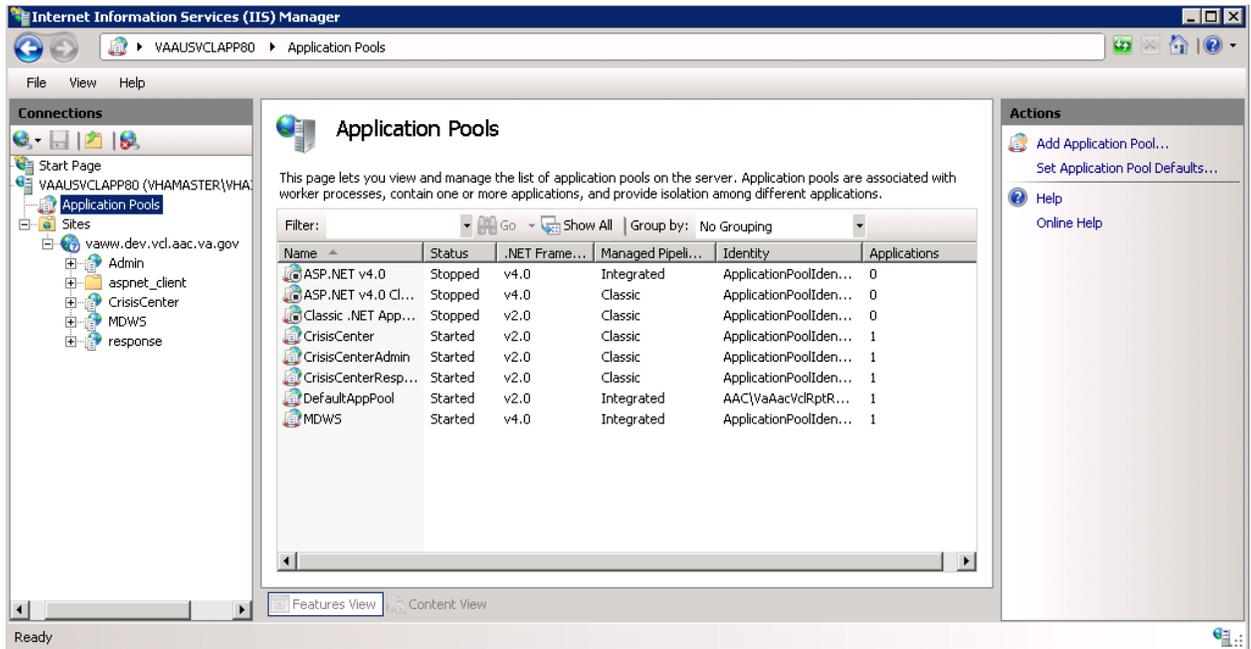


Figure 11: Application Pools

16. Double-click the CrisisCenter application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done
17. Double-click the Response application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done
18. Double-click the Admin application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done

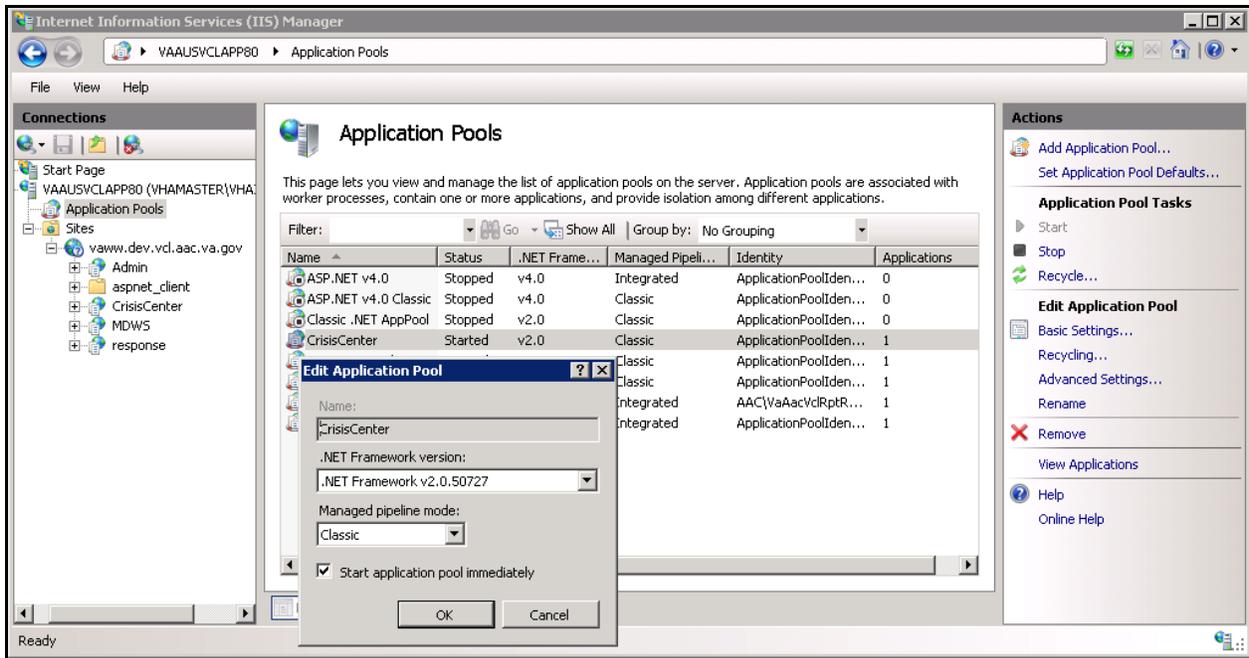


Figure 12: Edit Application Pool settings

CrisisCenter application pool permissions to the appropriate file system folder

19. Give the CrisisCenter application pool file system permissions to access the CrisisCenter code. Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenter folder, select Properties, and select the Security tab.

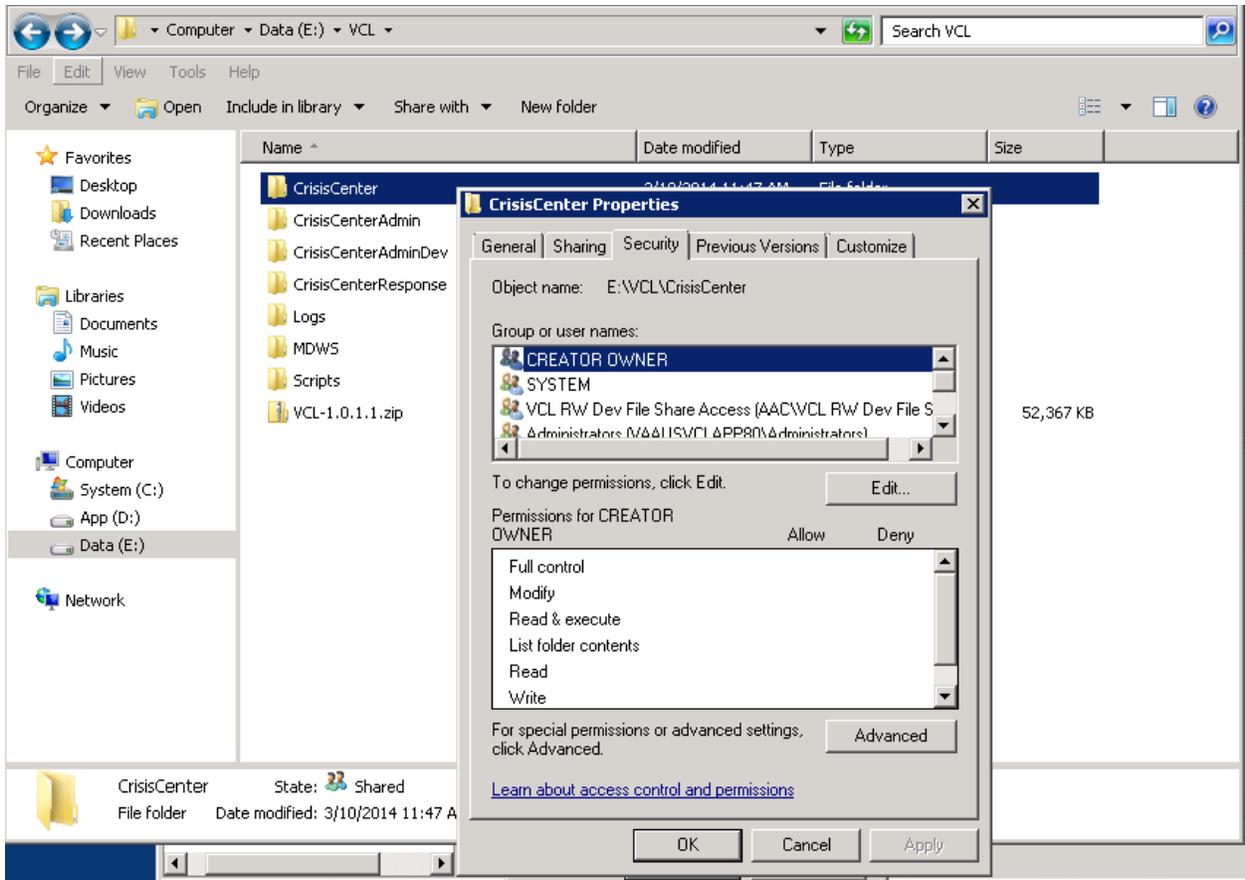


Figure 13: CrisisCenter Properties

20. Click the Edit button, then click Add.

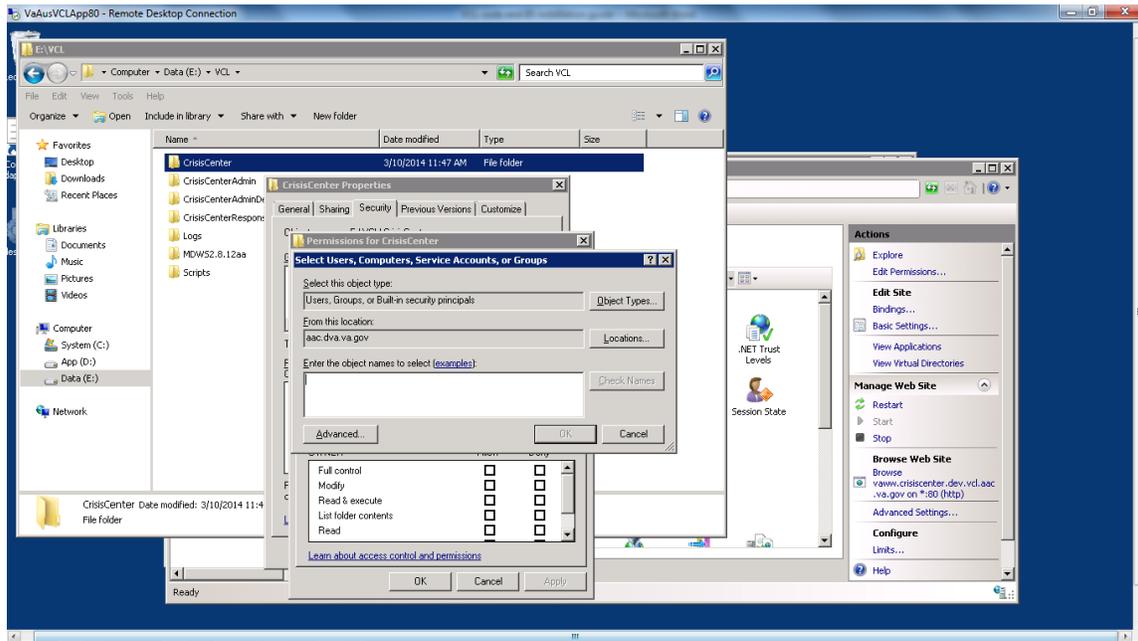


Figure 14: Permissions for CrisisCenter

21. Click Locations, and select the IIS server hosting the VCL code.

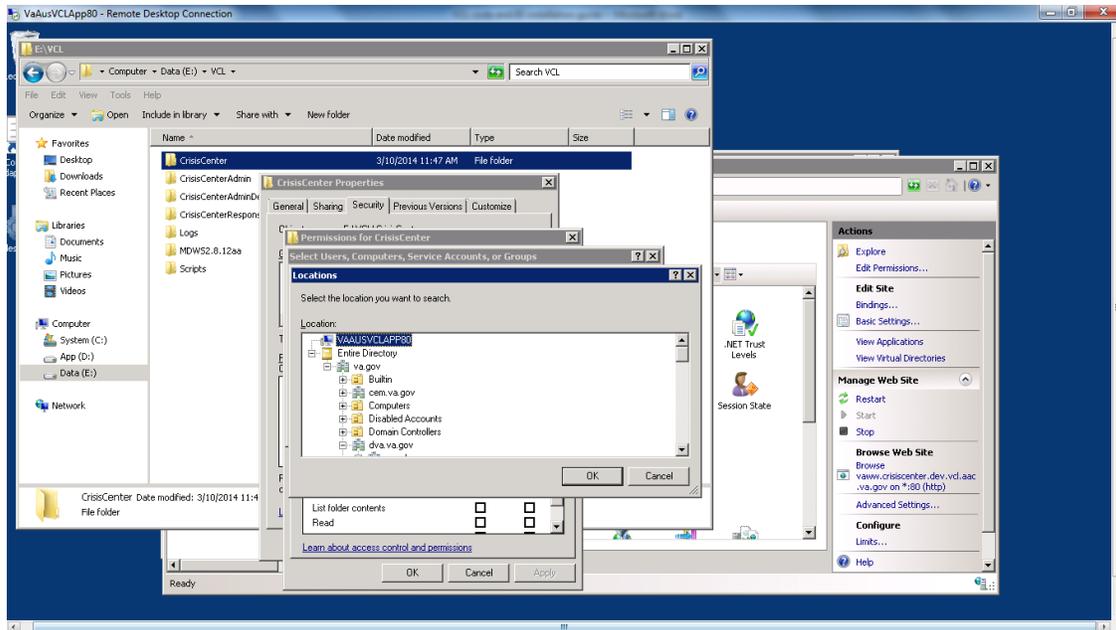


Figure 15: Locations

22. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\CrisisCenter” for the CrisisCenter website.

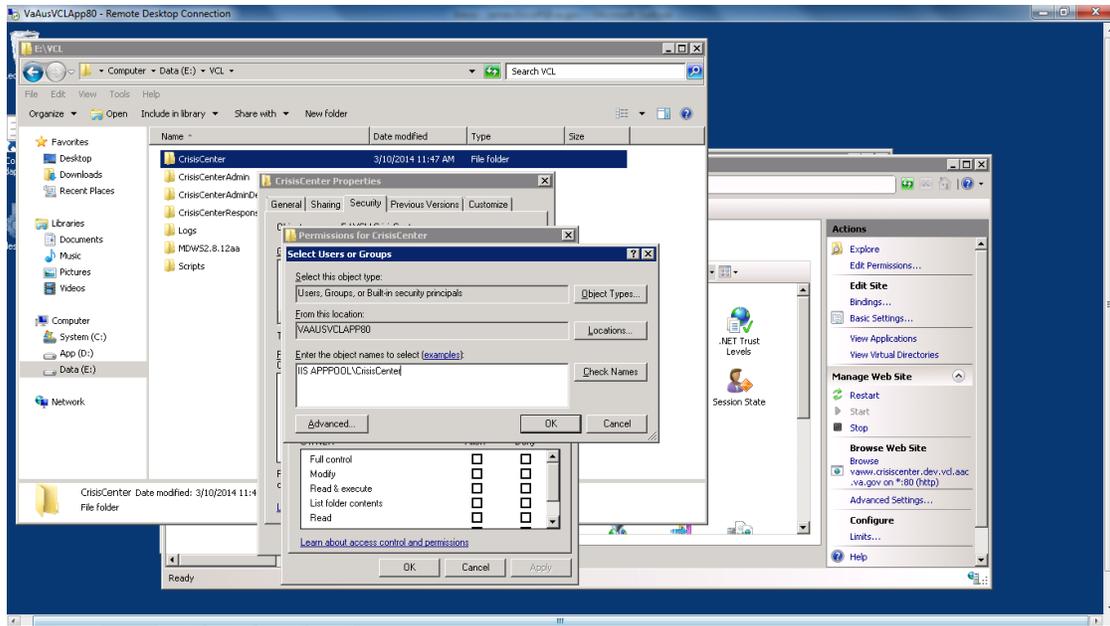


Figure 16: Enter the Object Names to Select

23. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.

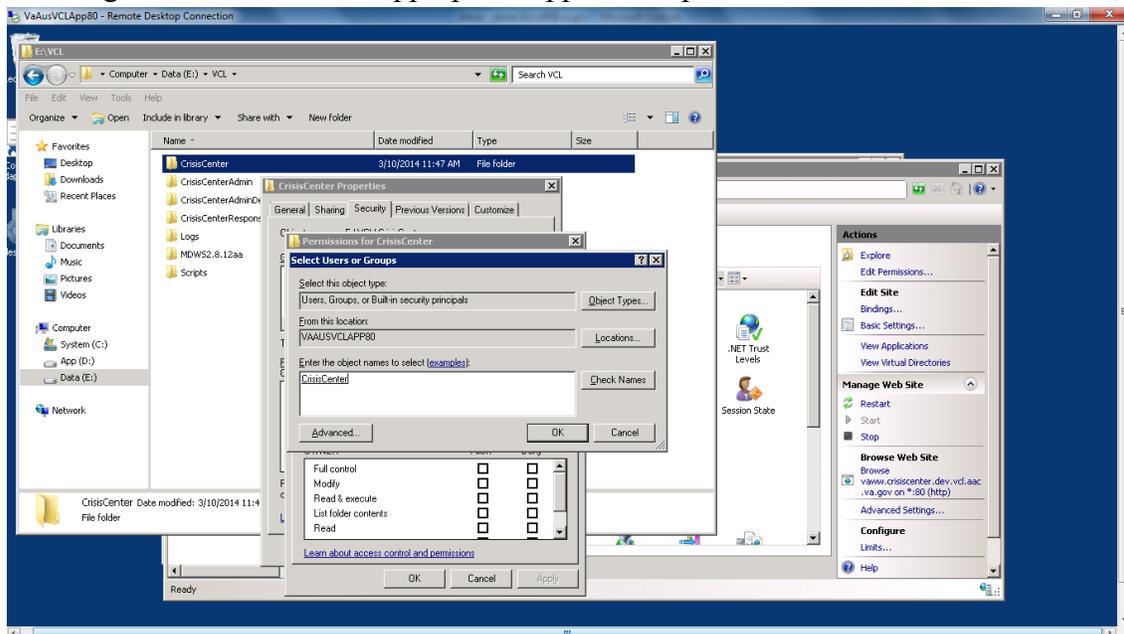


Figure 17: Check Names

24. Click OK. Leave the default permissions granted to the application pool account.

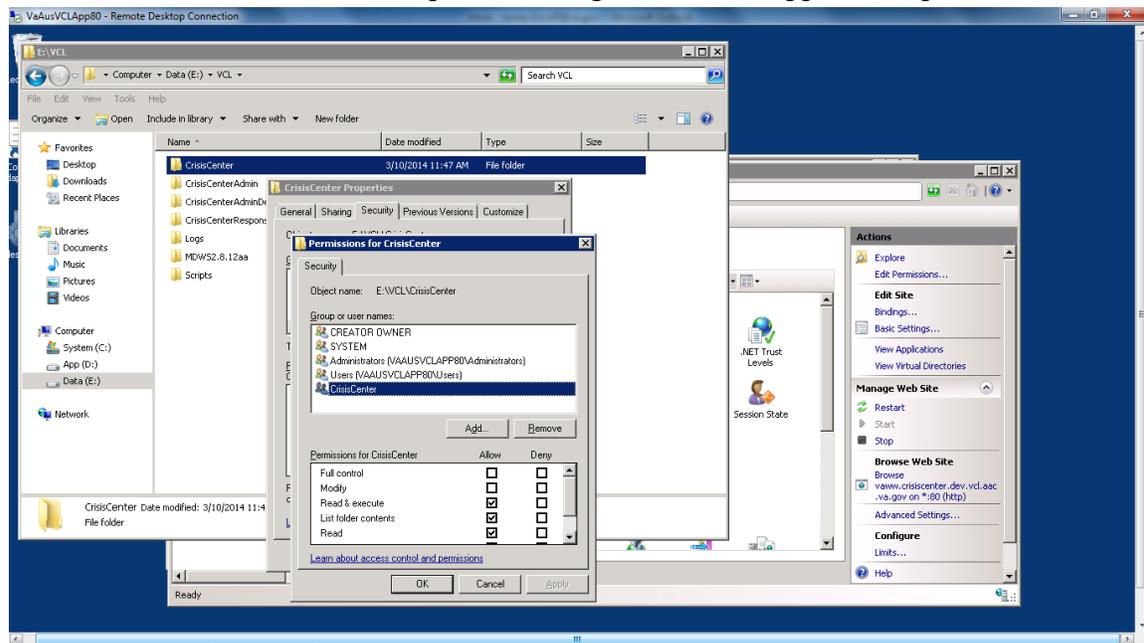


Figure 18: Default Permissions

25. Click OK until all folder property windows are closed.

Admin application pool permissions

26. Give the Admin application pool file system permissions to access the Admin code.
Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenterAdmin folder, select Properties, and select the Security tab.
27. Click the Edit button, then click Add.
28. Click Locations, and select the IIS server hosting the VCL code.
29. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\Admin” for the Admin website.
30. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
31. Click OK. Leave the default permissions granted to the application pool account.
32. Click OK until all folder property windows are closed.

Response application pool permissions

33. Give the Response application pool file system permissions to access the Response code. Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenterResponse folder, select Properties, and select the Security tab.
34. Click the Edit button, then click Add.
35. Click Locations, and select the IIS server hosting the VCL code.
36. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\Response” for the Response website.
37. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
38. Click OK. Leave the default permissions granted to the application pool account.
39. Click OK until all folder property windows are closed.

Web site IIS authentication pass-through settings.

40. In IIS Manager, select the CrisisCenter virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.

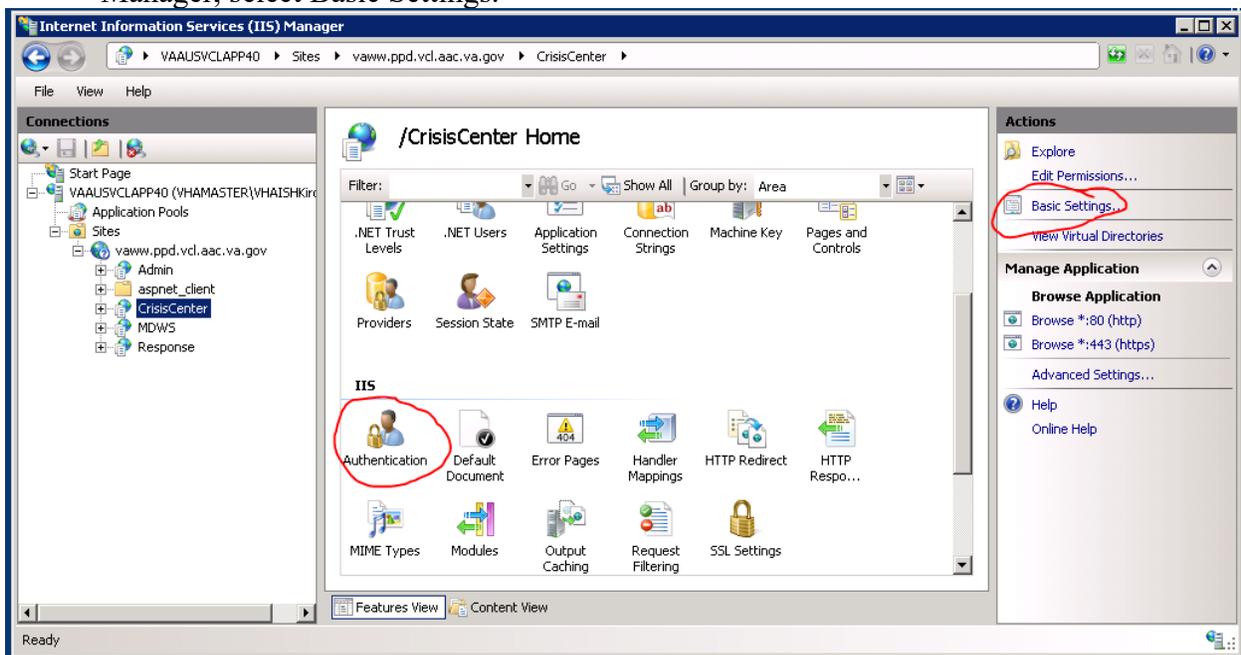


Figure 19: IIS Manager, CrisisCenter Virtual directory

41. Click Connect As.

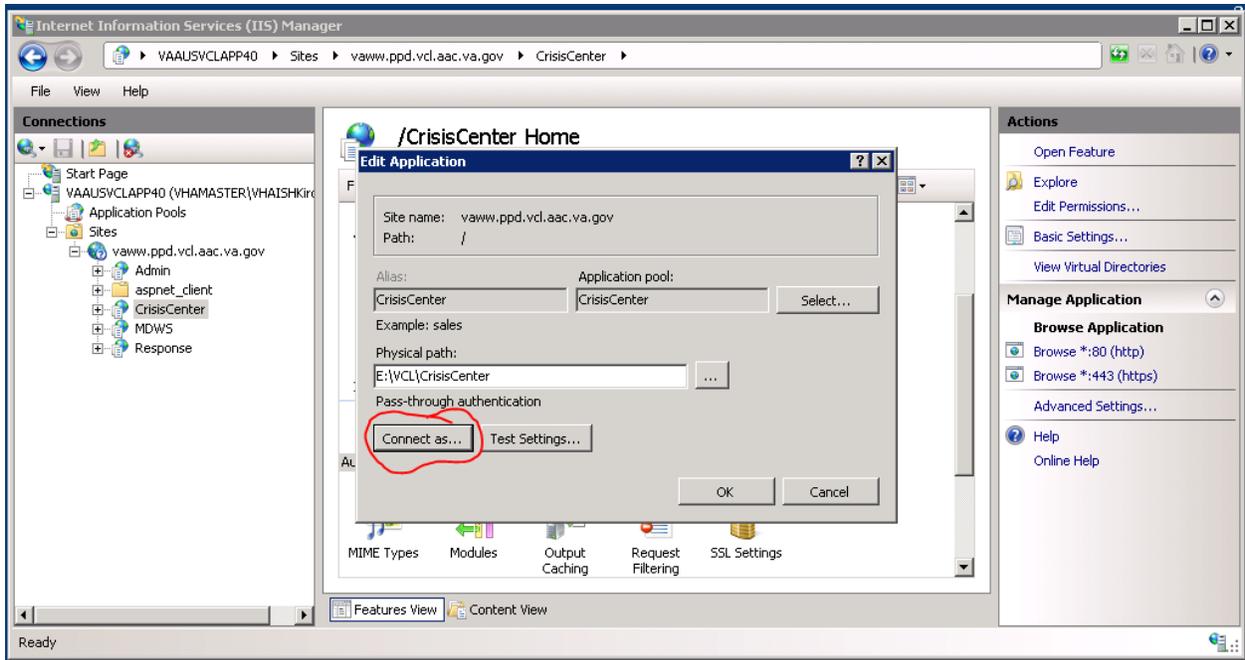


Figure 20: Edit Application

42. Select “Application user (pass-through authentication).”

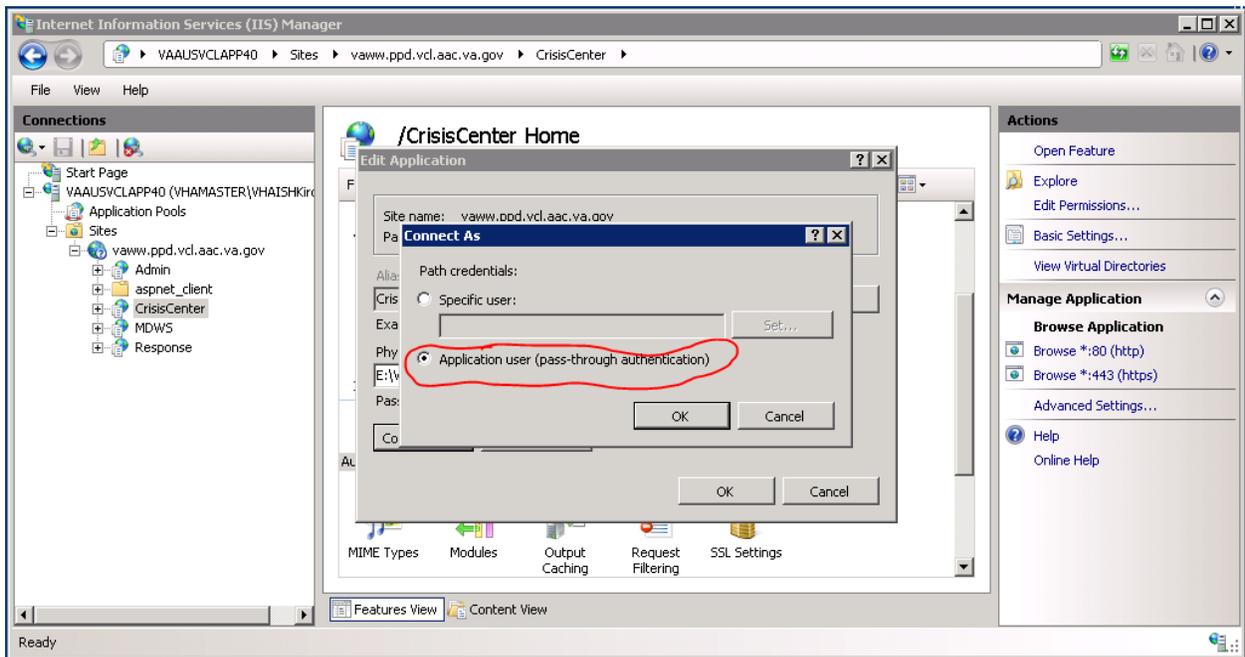


Figure 21: Connect As dialogue

43. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.

44. In IIS Manager, select the Admin virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.
45. Click Connect As.
46. Select “Application user (pass-through authentication).
47. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.
48. In IIS Manager, select the Response virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.
49. Click Connect As.
50. Select “Application user (pass-through authentication).
51. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.

Session state server set-up

- 52.

Web site set up verification

Note: The following are links for pre-production and production environments:

Dev

REDACTED

PreProd/Test

REDACTED

Prod

REDACTED

There are sub-sites in each environment:

For example, vcl.aac.va.gov/admin, vcl.aac.va.gov/crisiscenter, vcl.aac.va.gov/MDWS, and vcl.aac.va.gov/response.

53. Test each site out to see if they work properly. You will get screens like the following if the sites are working:

The screenshot shows a web browser window with the URL `http://crisiscenter.test.vcl.orl...` and the page title "Crisis Center". The interface is for the "crisis center HOTLINE" and includes the following elements:

- Navigation:** "Reports Menu" and "POIS Form" buttons in the top left.
- VISTA LOGIN:**
 - Select VISN: --Select VISN--
 - Select Site: --Select Site--
 - Access Code: [Text Input]
 - Verify Code: [Text Input]
 - Login: [Button]
 - Logout: [Button]
- VETERAN LOOKUP:**
 - Search MPI: [Text Input] [Search MPI Button]
 - Select State: [Dropdown]
 - Select Facility: [Dropdown]
 - Find Veteran: [Button]
 - Select Veteran: [Button]
- Acute Care Risk Assessment & Log Sheet:**
 - * = required field
 - IF SUICIDE ATTEMPT IS IN PROGRESS, ENACT CALL TRACE, CALL 911
 - Open All Panels: [Button]
 - RESPONSE INFO: [Dropdown]
 - Table with columns: Date/Time of call to hotline, Phone Station/Line*, Responder Name*, Source of Call*
 - Caller INFO: [Dropdown]
 - Caller Phone* (Red background), Caller Name* (Yellow background), Caller Is Veteran
 - Check for Prev. Calls: [Button]
 - Check If International #: [Checkbox]

Figure 22: Crisis Center Hotline Login

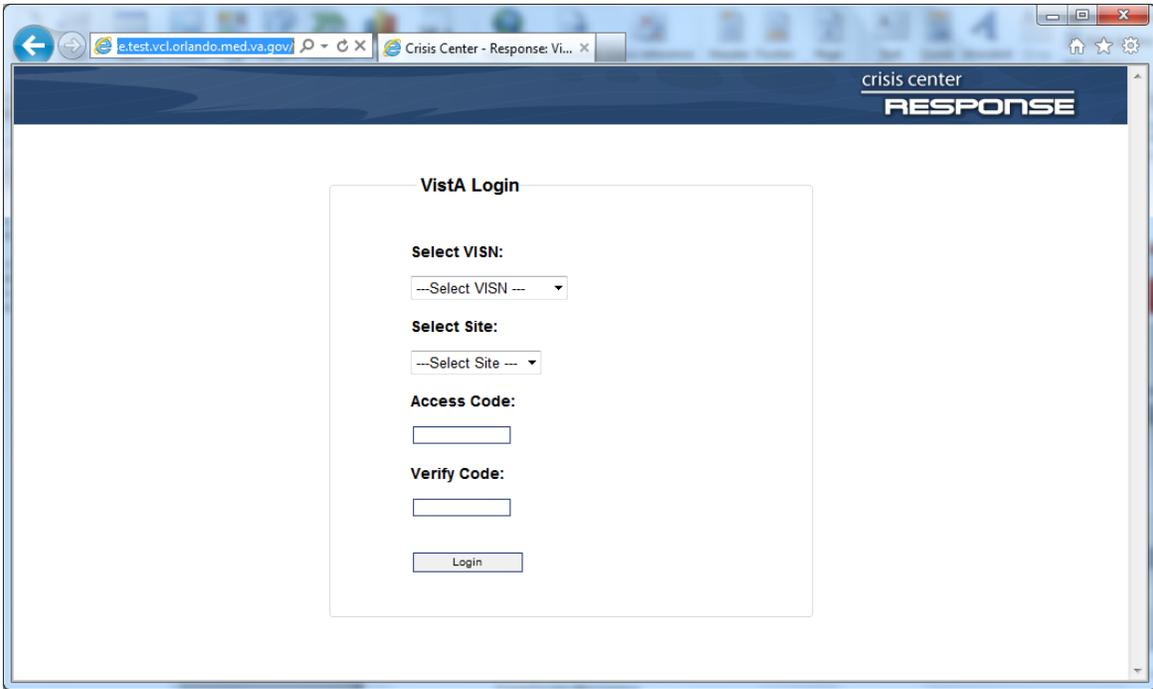


Figure 23: CrisisCenter Response

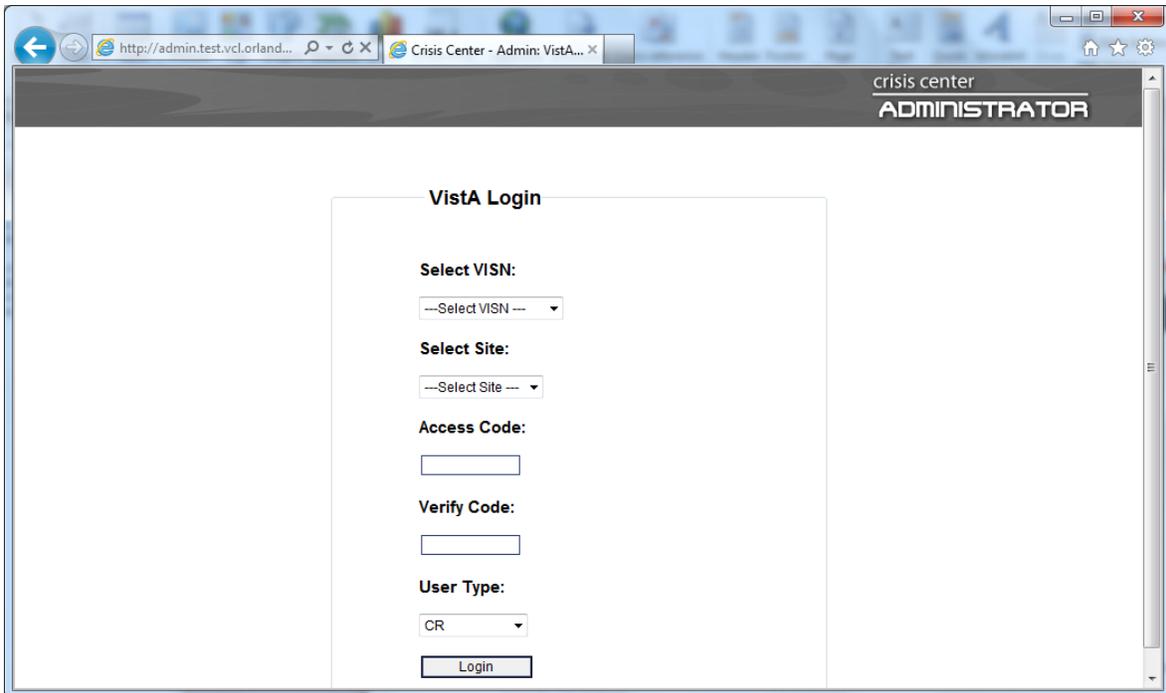


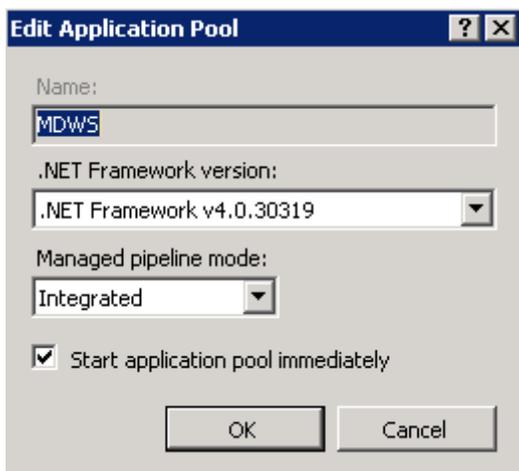
Figure 24: CrisisCenter Administrator

3.3. MDWS installation

MDWS is the web service application that bridge the gap between VCL applications and Vista sites. Current version used 3.0.3.5. The installation file is provided.

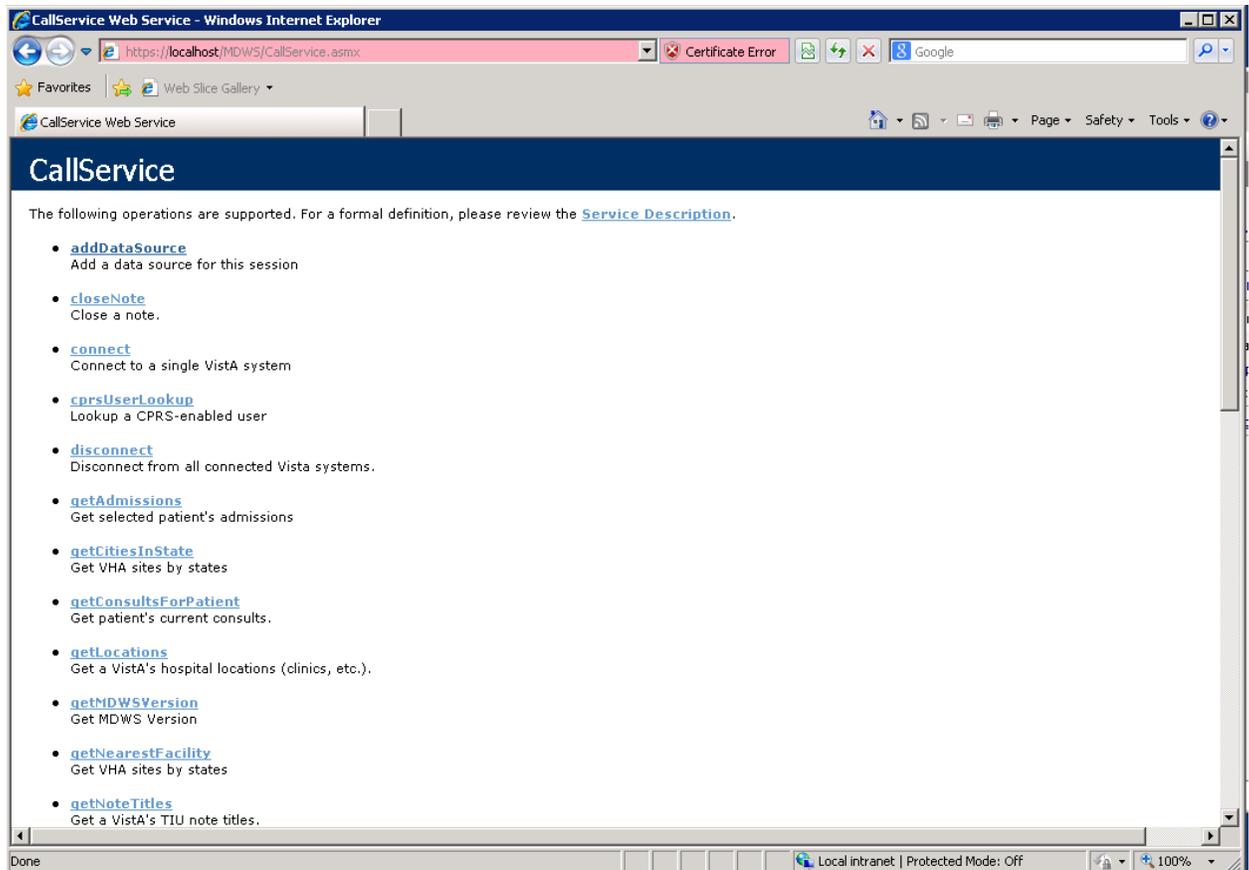
Installation Steps:

1. Verify the .NET Framework 4.0 is installed on the server. If not then install it.
2. Obtain the MDWS files from **REDACTED**.
3. Extract archive to E:\VCL\MDWS.
4. Open IIS Manager and select Application Pools.
5. Create an application pool with the following parameters:



6. Under Sites, right click the server website name and select Add Application.
7. Fill in the following information for the MDWS web application:
 - a. Site name: MDWS
 - b. Application pool: MDWS
 - c. Physical path: E:\VCL\MDWS
8. Set up the session state server for MDWS by going to the server website/MDWS Home - > ASP.NET, then double-click Session State.
9. Under Session State, select In Process, and then click Apply
10. Give the MDWS application pool file system permissions to access the MDWS code. Open Windows Explorer, navigate to E:\VCL\, right-click the MDWS folder, select Properties, and select the Security tab.
11. Click the Edit button, then click Add.
12. Click Locations, and select the IIS server hosting the MDWS code.

13. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\MDWS” for the MDWS website.
14. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
15. Click OK. Leave the default permissions granted to the application pool account.
16. Click OK until all folder property windows are closed.
17. Once completed, test it going to <https://localhost/MDWS/CallService.asmx> in a browser on the server.



Obtaining the VCL Installation Files

- The VCL application code will be provided in a ZIP archive. This archive is to be unpacked in the directory that will host the three websites needed for VCL: Hotline, Response, and Admin. The lead developer of the VCL team will have the location of the archive of the code files. These files will be uploaded into `vaauvclapp80\vcl` into a file name that includes software version information
- The VCL database installation is performed by restoring from a SQL Server backup file. The details regarding file name and location should be available with the Database Administrator. (Dev and PPD data exports will be uploaded into

vaausvclapp80\vcl. PRD data transfer will be accomplished according to the separate Data Transfer Agreement.)

Perform a restore for the VCL database, using the appropriate backup file. A sample restore statement is provided below:

```
RESTORE DATABASE [NationalSuicideHotline_PreProd] FROM
DISK = N'C:\0_VCL\TEMPDB-Backup'
WITH FILE = 1,
MOVE N'NationalSuicideHotline' TO
N'C:\0_VCL\PreProd\NationalSuicideHotline_PreProd_dat.mdf',
MOVE N'NationalSuicideHotline_log' TO
N'C:\0_VCL\PreProd\NationalSuicideHotline_PreProd_log.ldf',
NOUNLOAD,
STATS = 10
GO
```

3.4. System Requirements

Storage requirements for installation:

Type of Data	Size
Applications	< 5MB
Help Files	< 1MB

Sites should reserve 1KB of storage space per observation for data that will accumulate. The vast majority of growth will occur in the OBS file (#704.117).

The following describes the installation environment for on the VistA client workstation:

- Workstations must be running under Windows. Refer to <http://vaww.vairm.vaco.va.gov/vadesktop> for additional information on VA standard desktop configurations.
- Remote Procedure Call (RPC) Broker Workstation must be installed.
- The workstation must be connected to the local area network.
- Administrator privileges are needed on any machine on which CP Gateway Service is installed.

4. Backout Plan

This section outlines the back out procedures for VCL.

During installation of a new VCL baseline, if there are any issues with new baseline, the new baseline will be backed out and the system will be restored to the previous baseline.

In the event that a backout of the VCL installed code is needed, code should be rolled back to the last known working version. AITC will retrieve the tape backup of the last known good production version to reinstall. The database admin and system admin will determine the correct last working version to rollback to.

The following are the steps to back out VCL to its previous version:

1. Notify the **Remedy Help Desk** **REDACTED** and VCL application users about backout plan initiation.
2. When VCL is first deployed to AITC, a copy of the existing VCL install files will be placed at **vaausvclapp80\vcl**.
3. Disable user access to the VCL system while the back out procedures are in process.
4. Delete all of the VCL code from the following location where it was uploaded onto the dev server:

vaausvclapp80\vcl\vcl-2.0 build 21.zip (Build information is provided as an example.)

The VCL code will be in an archive, with a naming convention that identifies the version, and when unpacked will have a directory structure similar to the following:

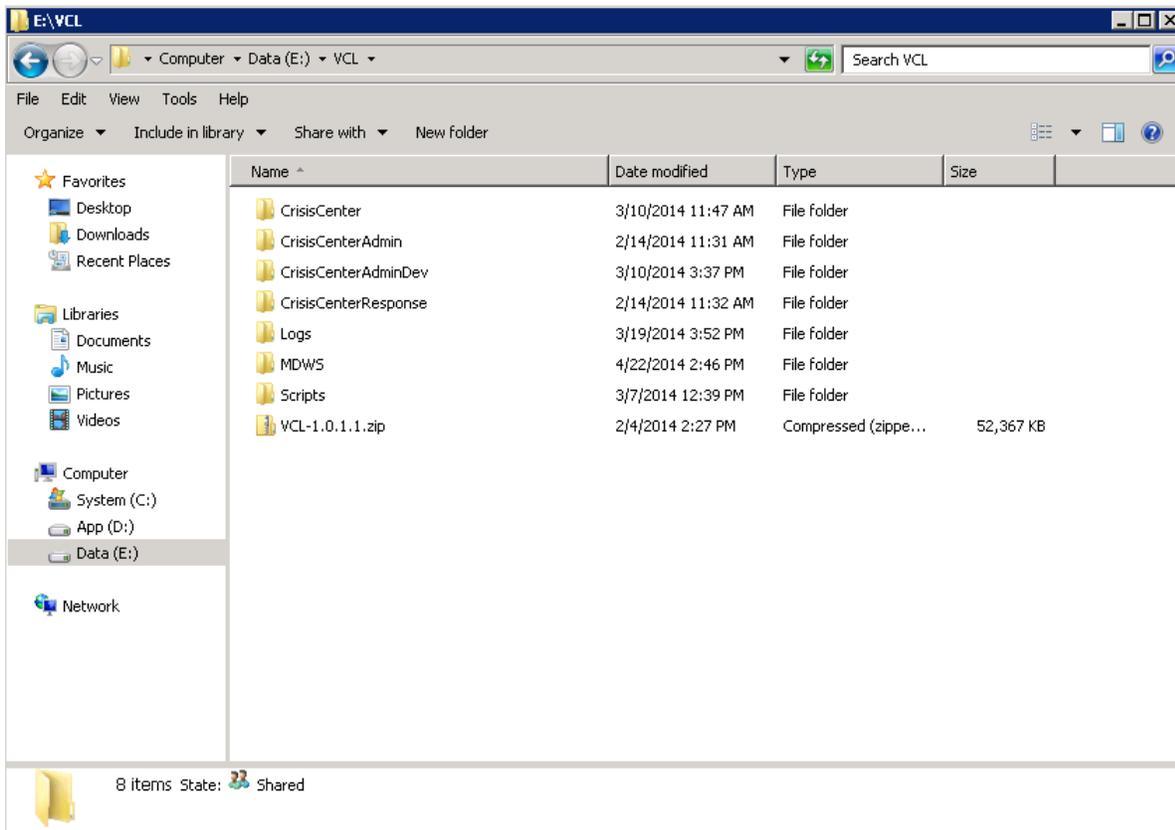


Figure 25: Unpack VCL Code Archive

5. Rename the backup copied folders. Backup the VCL database on the dev server (**vaussql1a**.)
6. Perform a full database backup of database "**NationalSuicideHotline_Test**" on **vaussql1a**.
7. Create an additional backup VCL folder at an additional location on **vaussql1a** in case the VCL application needs to be backed out again.
8. Conduct system health checks of the VCL application.
9. Enable VCL application user access.
10. Notify the **Remedy Help Desk** (1-888-596-4357) and VCL users of successful backout.

5. Post Installation Instructions

The AITC Build Manager will submit the needed access request forms (if not already submitted) for the environment. Where possible, a primary POC for each group of permissions being granted will be designated. The System and Database Administrators will complete the SDM tasks needed to grant access as required. The primary POC for each group should be contacted to verify access.

Note: *This Install Guide Addresses the basic "vanilla" product.*

After completing the instructions contained in this Guide, please apply the Patch in order to upgrade the product to the latest version. We need to include the all the Increment 3 upgrades.

Instructions for the Patch, along with the step-by-step database scripts, have been detailed in change order CO217347FY14.

6. Installing and Configuring the SQL Server Reports Server (SSRS) Component

This section is intended to provide a complete step-by-step walkthrough for installing and configuring the SQL Server Reports Server component, for the Veterans Crisis Line application.

6.1. Audience

The intended audience is the System and Database Administrators, and the VCL Manager at AITC.

6.2. Pre-Requisites

The following pre-requisites must be in place before all the steps outlined in this document can be completed:

1. Two security groups will need to be setup in the VA Active Directory:
 - VCL REPORTVIEWER and VCL REPORTMANAGER.

The Group creation process is as follows:

- First create the Group in the VA active directory
 - Next create a *database login* for the Group, in the NationalSuicideHotline database
 - Then create a *user* corresponding to the *login*, in the ReportServerDatabase.
 - Finally, add the authorized individuals, as members of the group.
 - **Notes:**
 - a. The suffixes *_DEV* and *_PPD* must be added to these groups, in order to set them up for the Development and Preproduction environments respectively.
 - b. Group membership is controlled through the AITC user creation process. A “VA 9957” security form must be processed for each member who is added to the group.
2. A “service account” will need to be setup for each environment:
(For the DEV, Pre-Prod and Prod databases, respectively)
 - i. Dev
 1. VaAacVclAppDev - Development Application Service Account
 2. VaAacVclRptRODev - Development Reporting Service Account
 - ii. Preproduction
 3. VaAacVclAppPpd - PreProduction Application Service Account

- 4. VaAcVclRptROPpd - PreProduction Reporting Service Account
- iii. Production
 - 5. VaAcVclAppPrd - Production Application Service Account
 - VaAcVclRptROPrd - Production Reporting Service Account

The service account creation process is as follows:

- o First create the account in the VA active directory
- o Next create a **database login** in the NationalSuicideHotline database
- o Then create a **user** corresponding to the login, in the ReportServerDatabase.
- o **Note:** This account must have read-only access to all the tables in the VCL Database, EXCEPT for: HotlineCalls, HotlineCalls_H, HotlineCallsDetails, HotlineCallsDetails_H.

6.3. Configuring the Reports Server (Includes SSL)

1. From the Start Menu, select “run as Administrator” for the Reporting Services Configuration Manager.

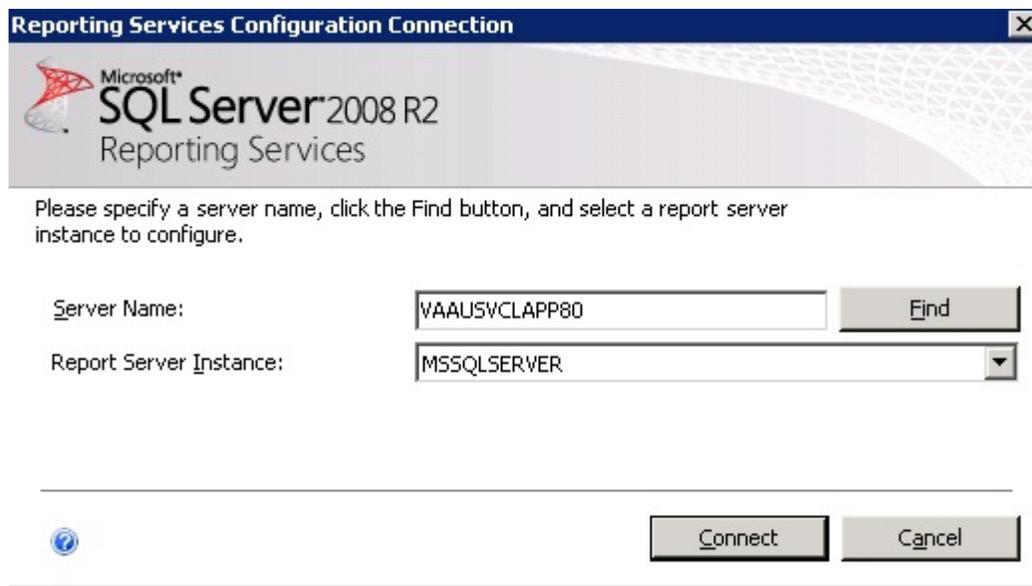


Figure 26: Reporting Services Configuration Connection

Here are the steps to configure SSL on SSRS:

Log on to VCL APP server → go to Reporting services configuration Manager, see below:

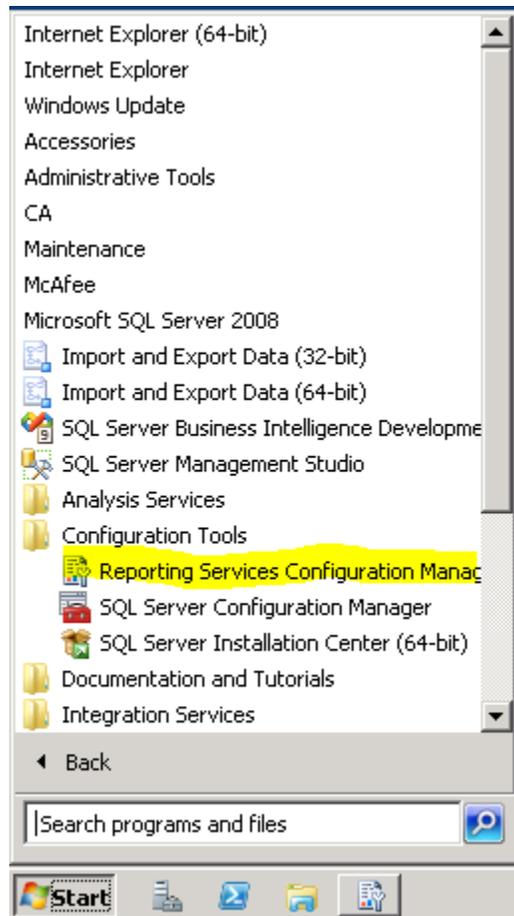


Figure 27: Reporting Services Configuration Manager

Click → window popup as below:

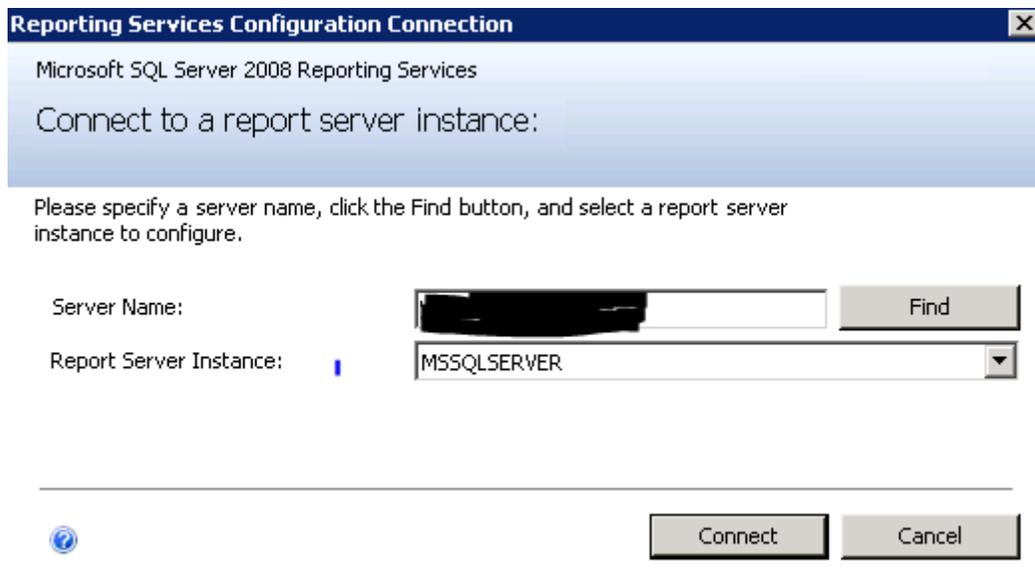


Figure 28: Specify a Server Name

Click Connect → see the above figure.

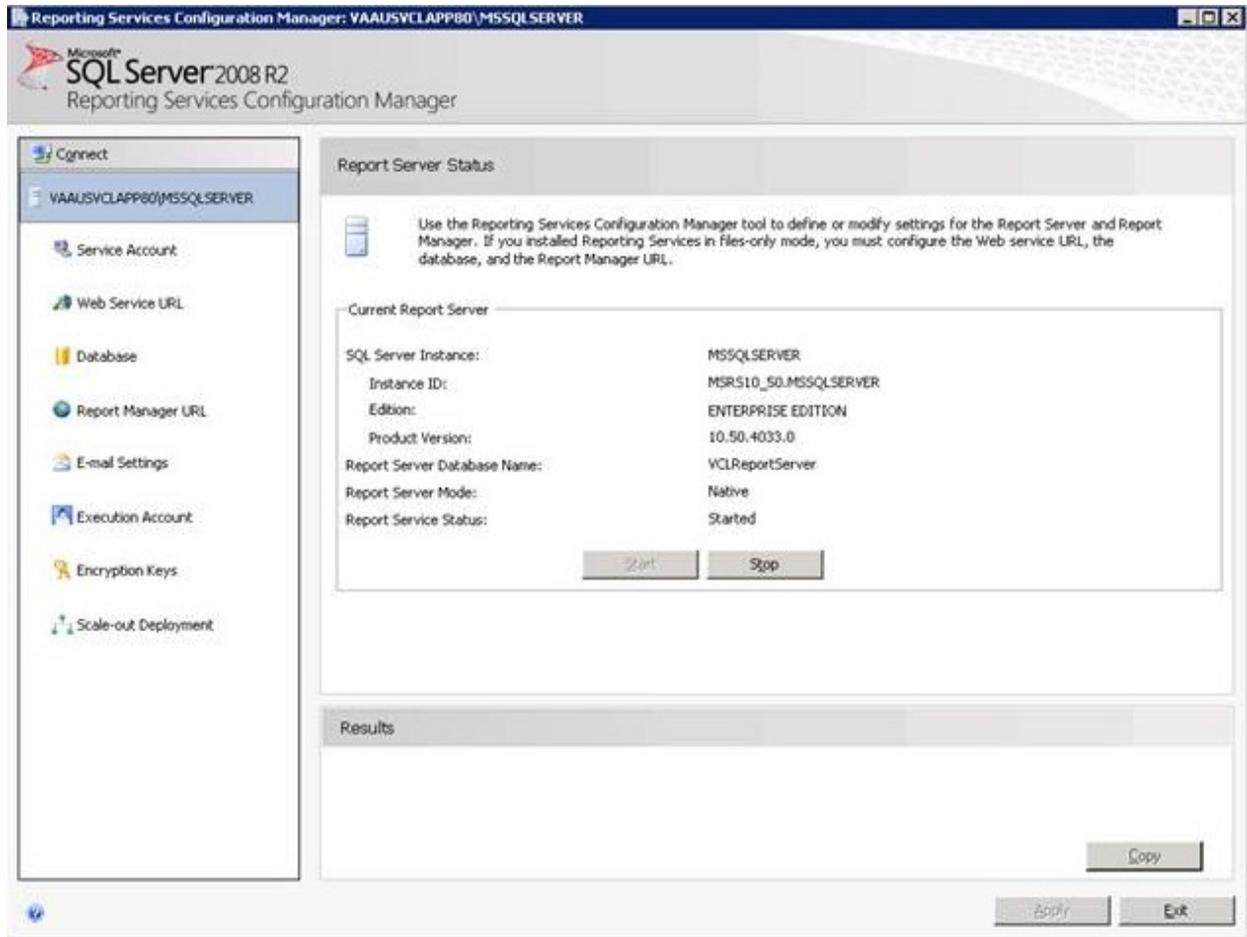


Figure 29: Report Server Status

Select Web services URL from the left-hand pane. Add the SSL certificate and SSL port (see drop-down highlighted in yellow.)



Figure 30: SSL Certificate and SSL Port

Click Advanced and add the following SSL Certificate information (highlighted in yellow below:)

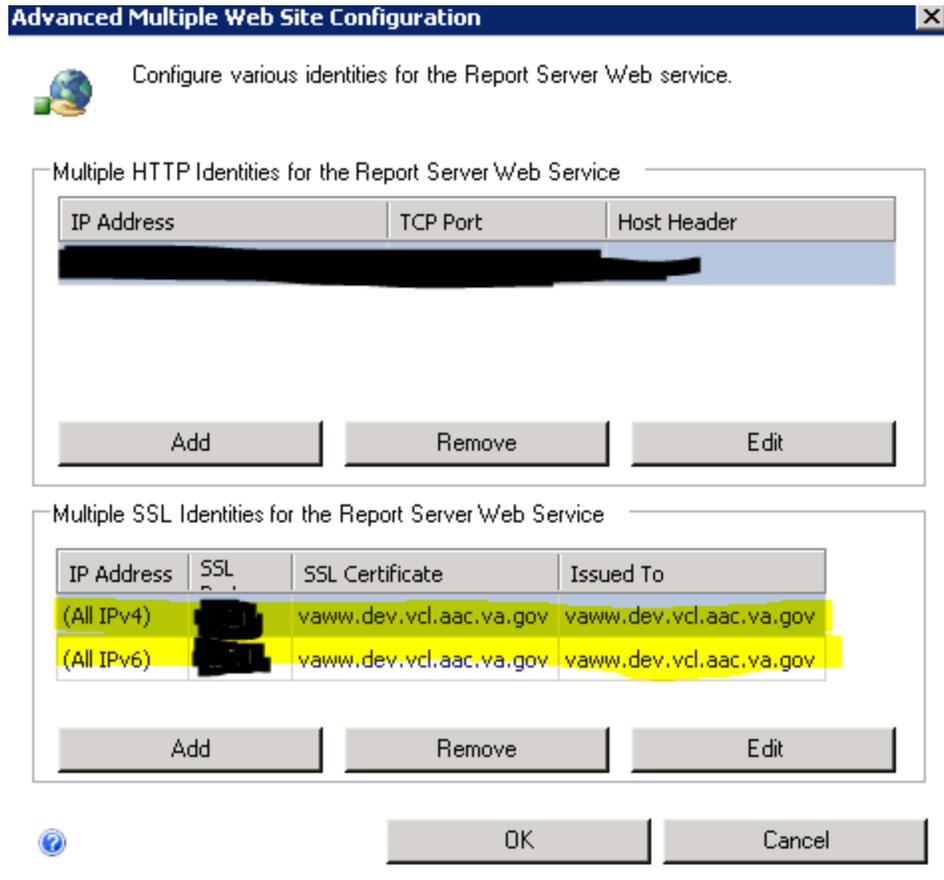


Figure 31: SSL Certification Information

Select the Report Manager URL

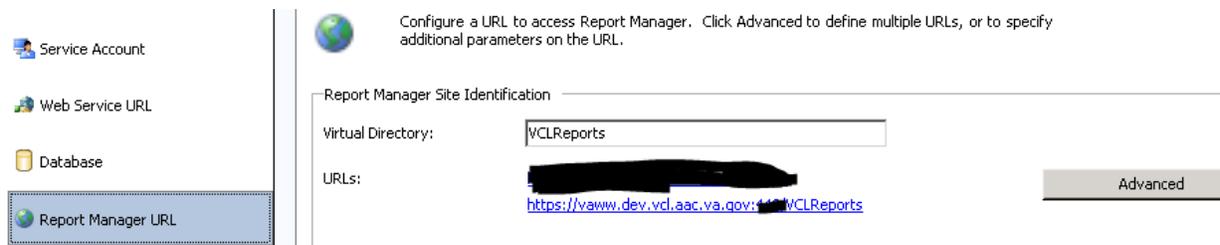


Figure 32: Add Report Manager URL

Click Advanced and add as shown below:

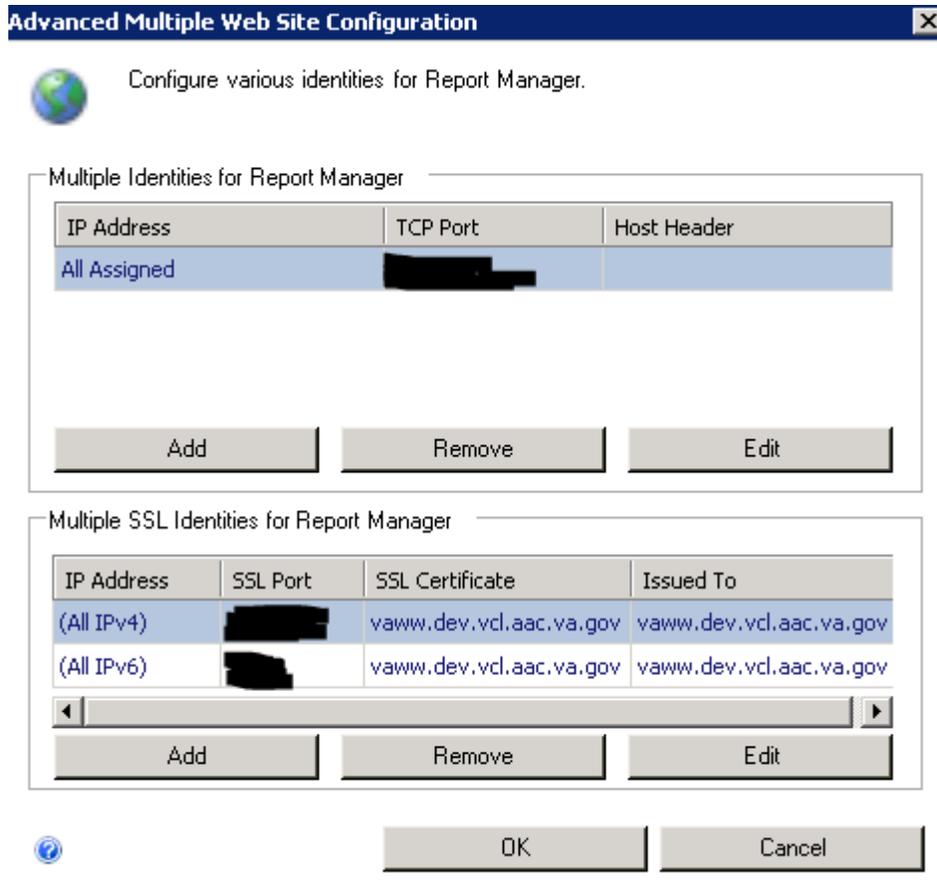


Figure 33: Updating SSL Certificates

Click OK.

This will complete the SSL section of SSRS.

6.4. Defining the Reporting Web Project

On the Application server machine (APP80 in case of Dev) open Internet Explorer and go to the reporting services URL.

1. From the Reports Manager home page, create a *Datasource* named VCLDatasource.

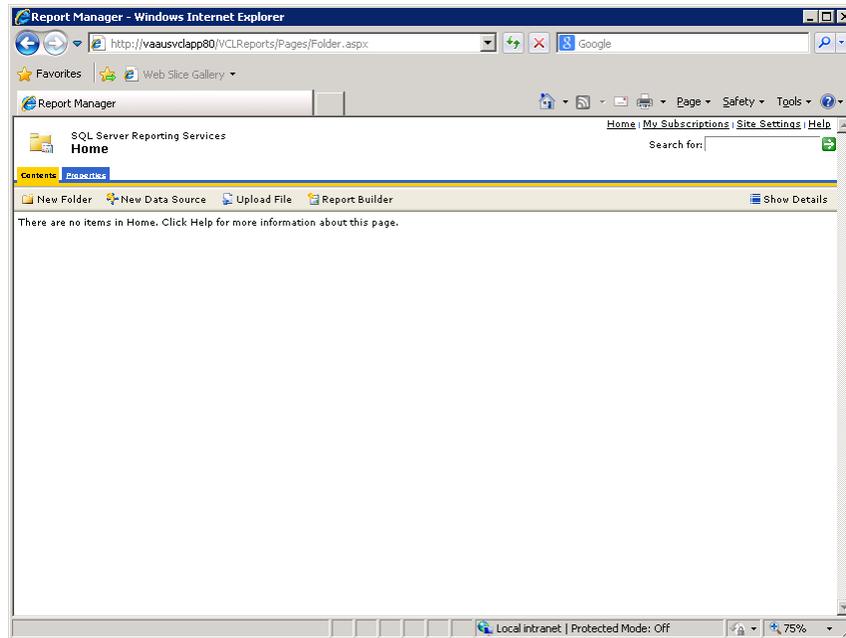


Figure 34: Create a Datasource

2. Select “Credentials stored securely in Reports Server”.

Also check “Use as Windows Credentials when connecting...”

Note: AITC will need to type in the username and password for the service account in this section.

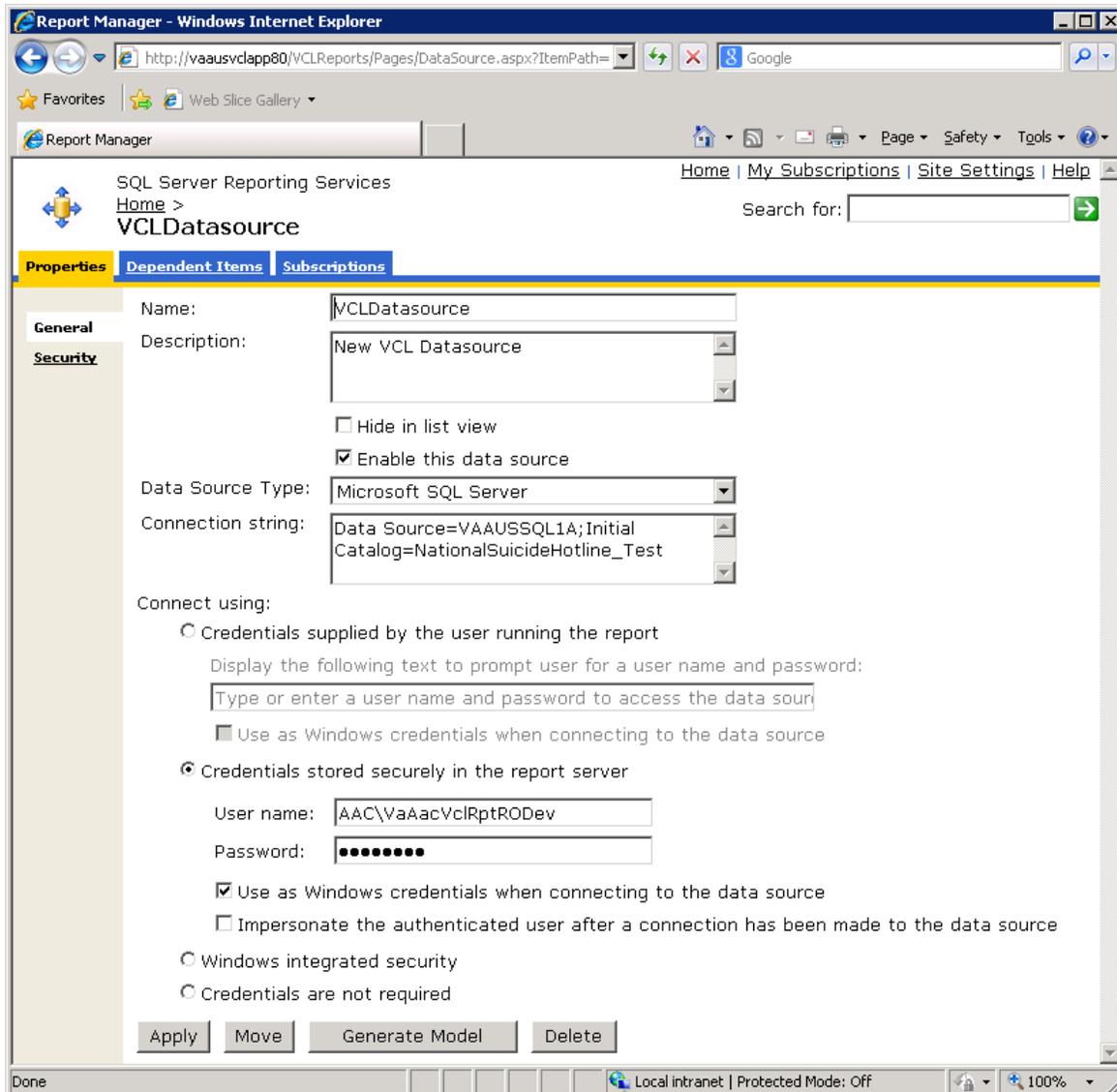


Figure 35: VCL Datasource

3. After the Datasource has been created, select it by clicking on it.
4. Click on Generate Model

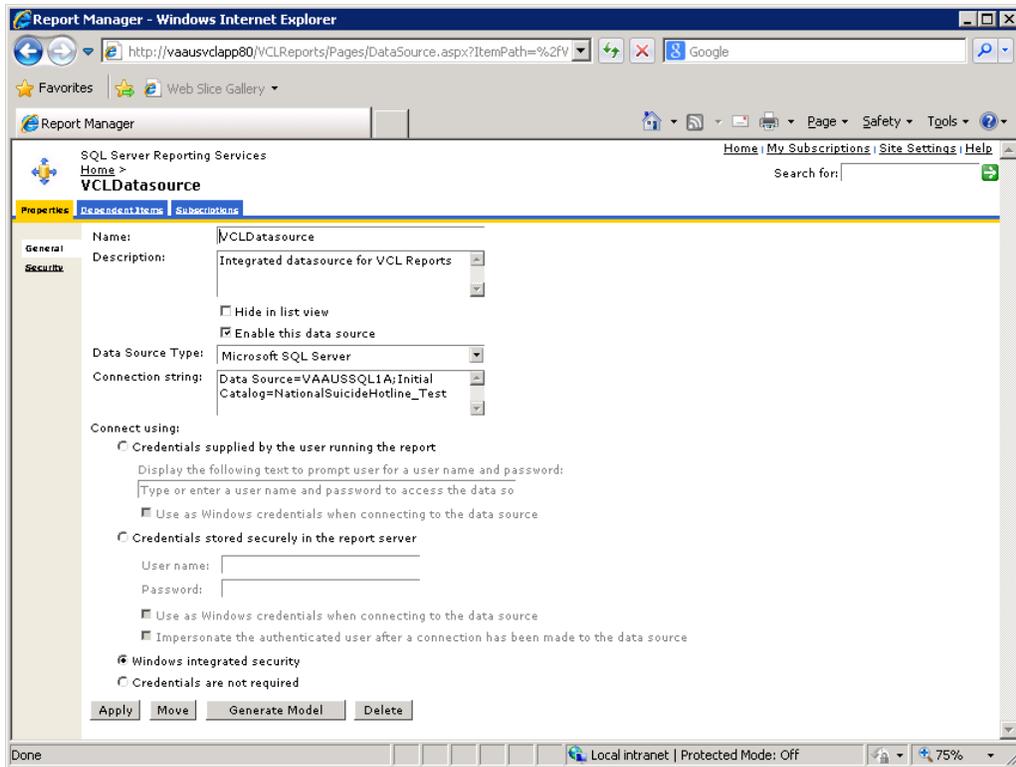


Figure 36: Generate Model

5. Create a new *Model* named VCLModel.

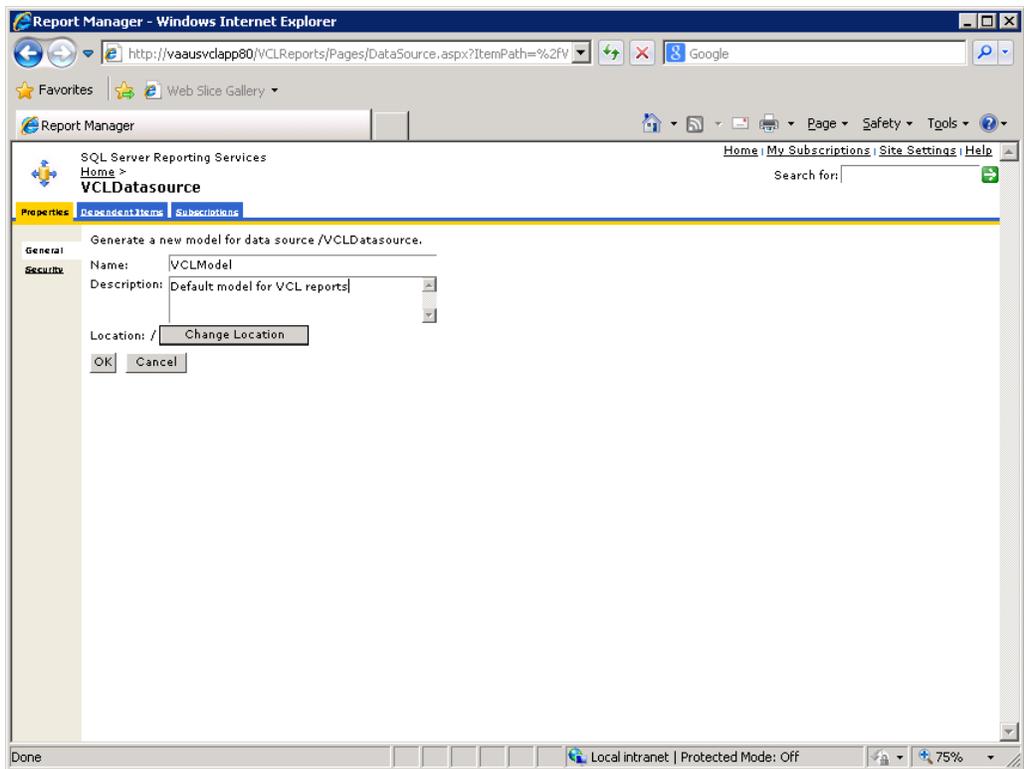


Figure 37: VCL Model

You must define the security, by adding role assignments and giving permissions.

6. To define the security, click on Site Settings.
7. Click New Role Assignment.
8. Add VCLREPORTMANAGER, as “System User” (allows Manager to see Report Builder link).

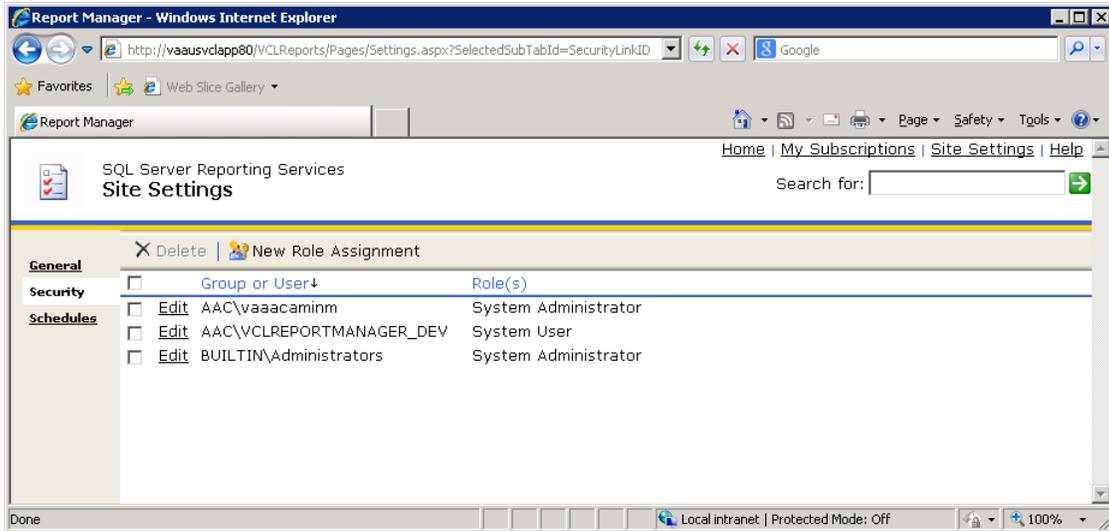


Figure 38: System User

Next, define the security for all the items that will be created.

9. Click the Home link, then Properties tab.
10. Click on **New Role Assignment**, add VCLReportManager and VCLReportViewer.

Manager gets Browser, Publisher and ReportsBuilder permissions. The Viewer group gets only Browser and Builder permissions.

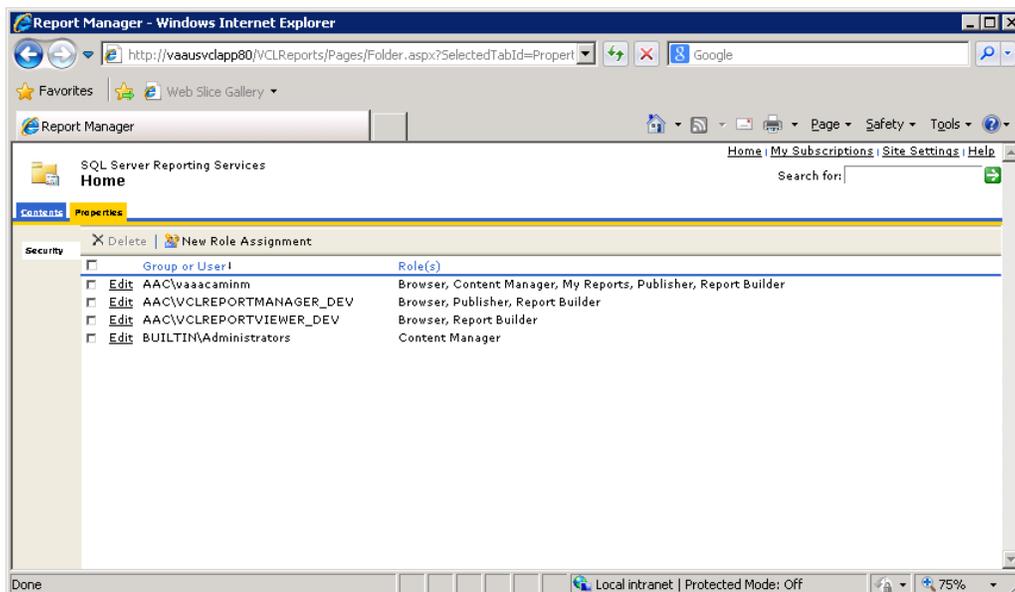


Figure 39: New Role Assignment

Next, ensure that the Datasource cannot be modified by anyone.

11. Click on the Datasource, and select the Security tab.
12. Ensure that even the MANAGER role can only see (but not alter) this particular object.

This is called Item-level security.

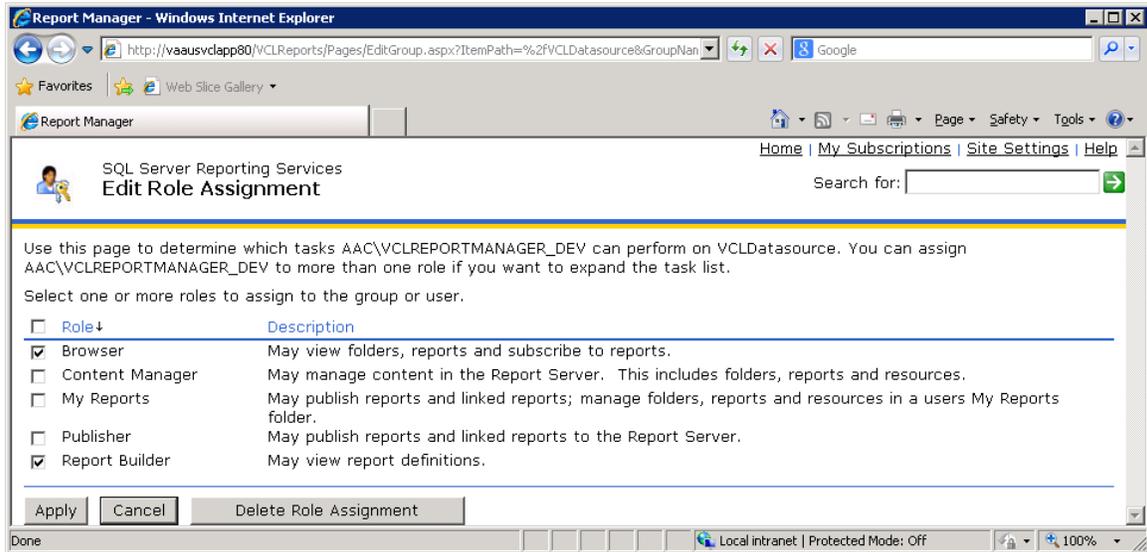


Figure 40: Edit Role Assignment

Similarly, you will want to override the inherited security for this item and set Item-level security for the Model as well:

13. Click on the Model, and select the Security tab.
14. Ensure that even the MANAGER role can only see (but not alter).

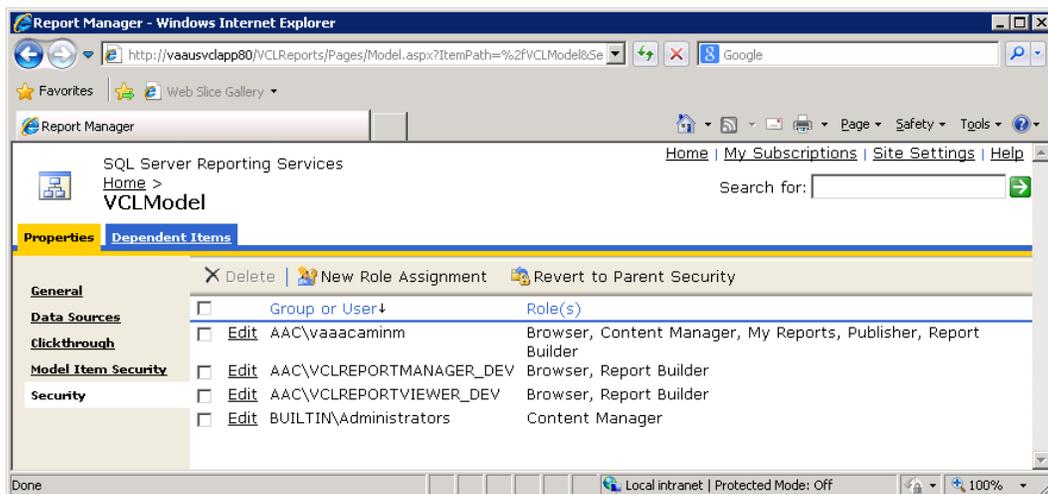


Figure 41: Security

15. Also, check the “Hide in List View” flag for the model. This will prevent its accidental deletion by the end user.

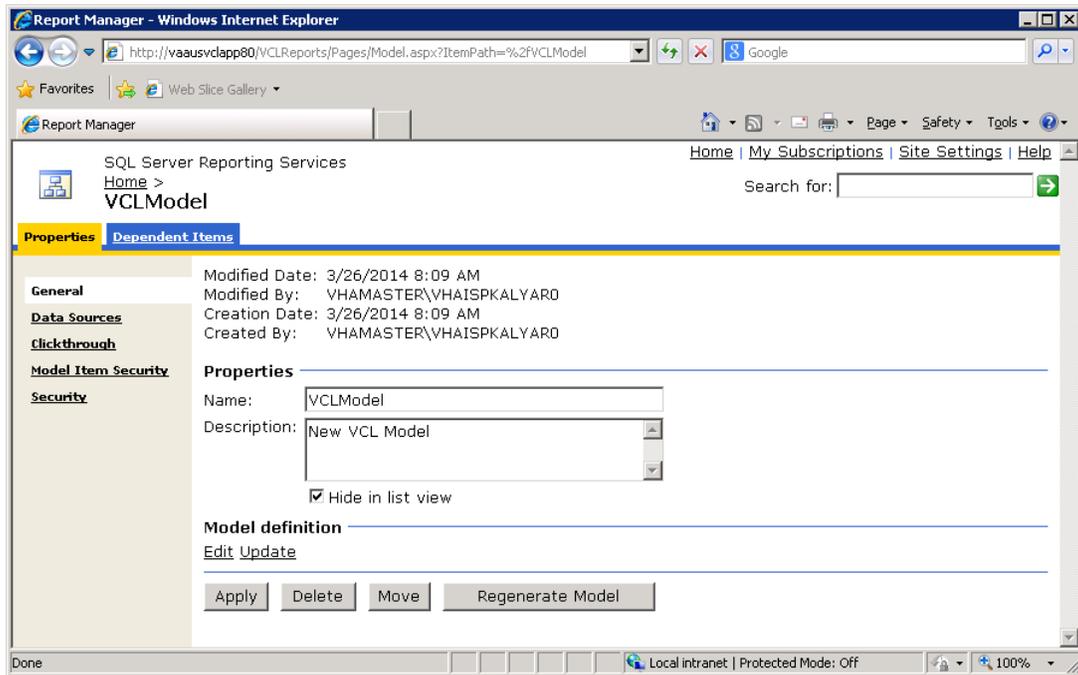


Figure 42: Properties

6.4.1. Customizing the Site name:

Click on Site Settings, then General. Enter the following text: Veterans Crisis Line – Custom Reports.

Note: Append (DEV) or (TEST) for those environments respectively.

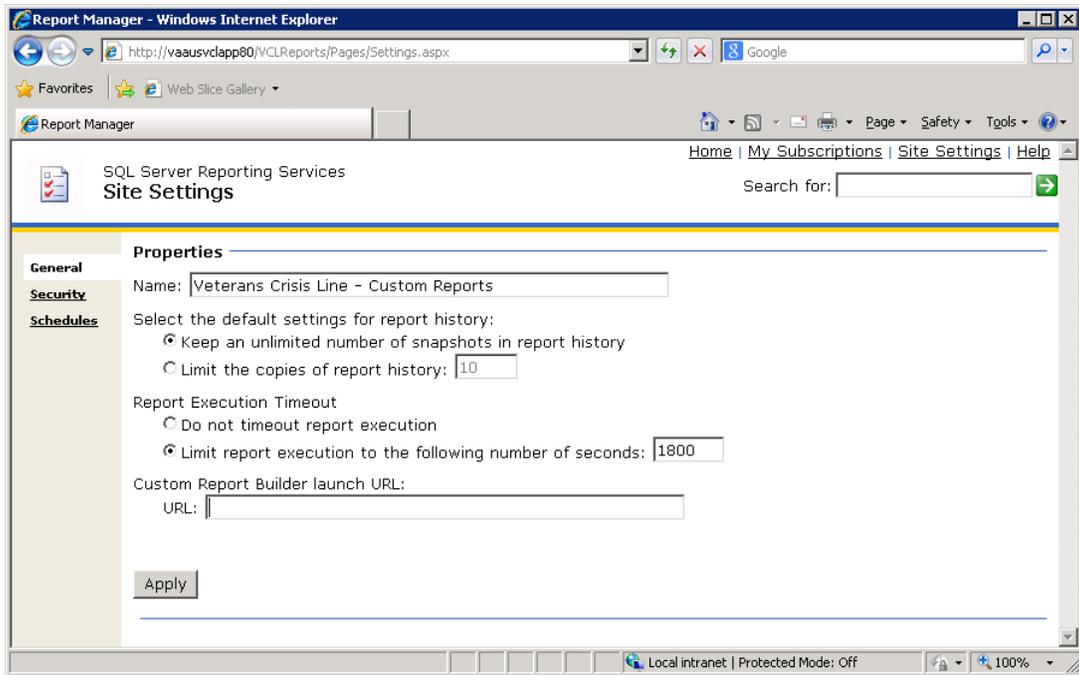


Figure 43: Veterans Crisis Line – Custom Reports

6.5. Reporting Services SSL Configuration

This has been covered in section 6.3

6.6. Uploading Previously Developed “Sample Reports” to the Server

On the Application server machine (APP80 in case of Dev) open Internet Explorer and go to the reporting services URL.

1. The pre-defined reports are located in the following folder on VaAusVclApp80 (the Dev Application Server):

E:\VCL\Scripts\Report_scripts

At the Reports Manager home page, select *Upload File* and upload the .rdl report files one by one.

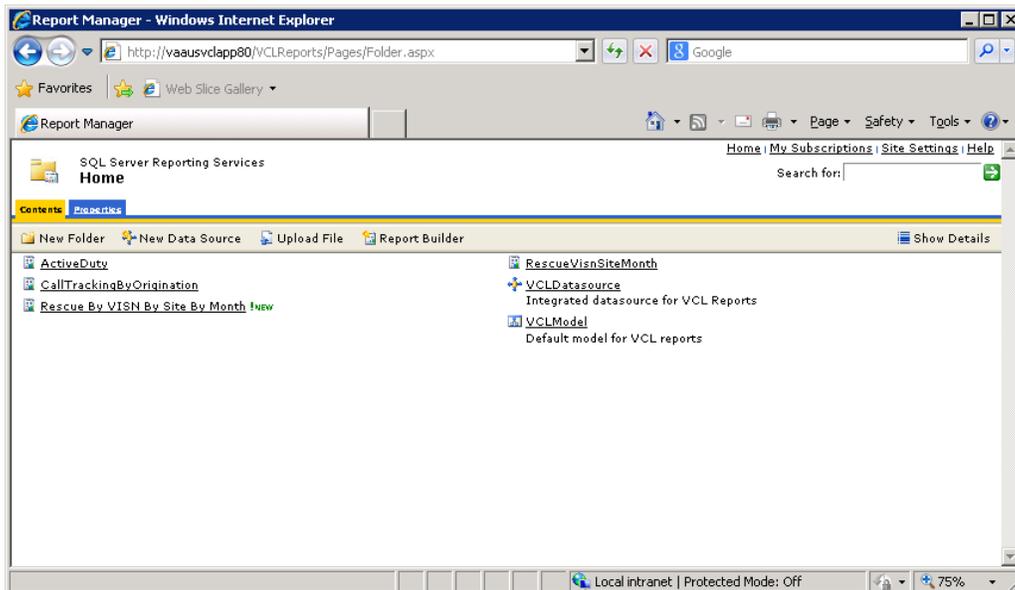


Figure 44: Upload File

7. Patching the Production Environment with Updated Code

In the event that a patch needs to be installed in the AITC production environment, the following steps should be followed.

1. Copy the patch files **REDACTED**
2. Write documentation that details how to install the patch. Use the following steps as a guideline. You may need to revise to meet your local environment specifications.
 - Open IIS Manager, expand Sites, and select the vaww.vcl.aac.va.gov website.
 - Under Manage Web Site, click Stop.
 - Copy code base archive **REDACTED** to production environment, and unzip.
 - Copy all files and folders from CrisisCenter to E:\VCL\CrisisCenter, overwriting existing files and folders.
 - Copy all files and folders from CrisisCenterAdmin to E:\VCL\CrisisCenterAdmin, overwriting existing files and folders.
 - Copy all files and folders from CrisisCenterResponse to E:\VCL\CrisisCenterResponse, overwriting existing files and folders.
 - Return to IIS Manager and click Application Pools.
 - Select the CrisisCenter application pool.
 - Under Application Pool Tasks, click Recycle.
 - Select the CrisisCenterAdmin application pool.
 - Under Application Pool Tasks, click Recycle.
 - Select the CrisisCenterResponse application pool.
 - Under Application Pool Tasks, click Recycle.
 - Under Sites, select vaww.vcl.aac.va.gov website.
 - Under Manage Web Site, click Start.
3. Send an email to the AITC team requesting a Change Order (CO) be opened for a patch be installed, and attach the installation instructions to the email. **REDACTED** For example:

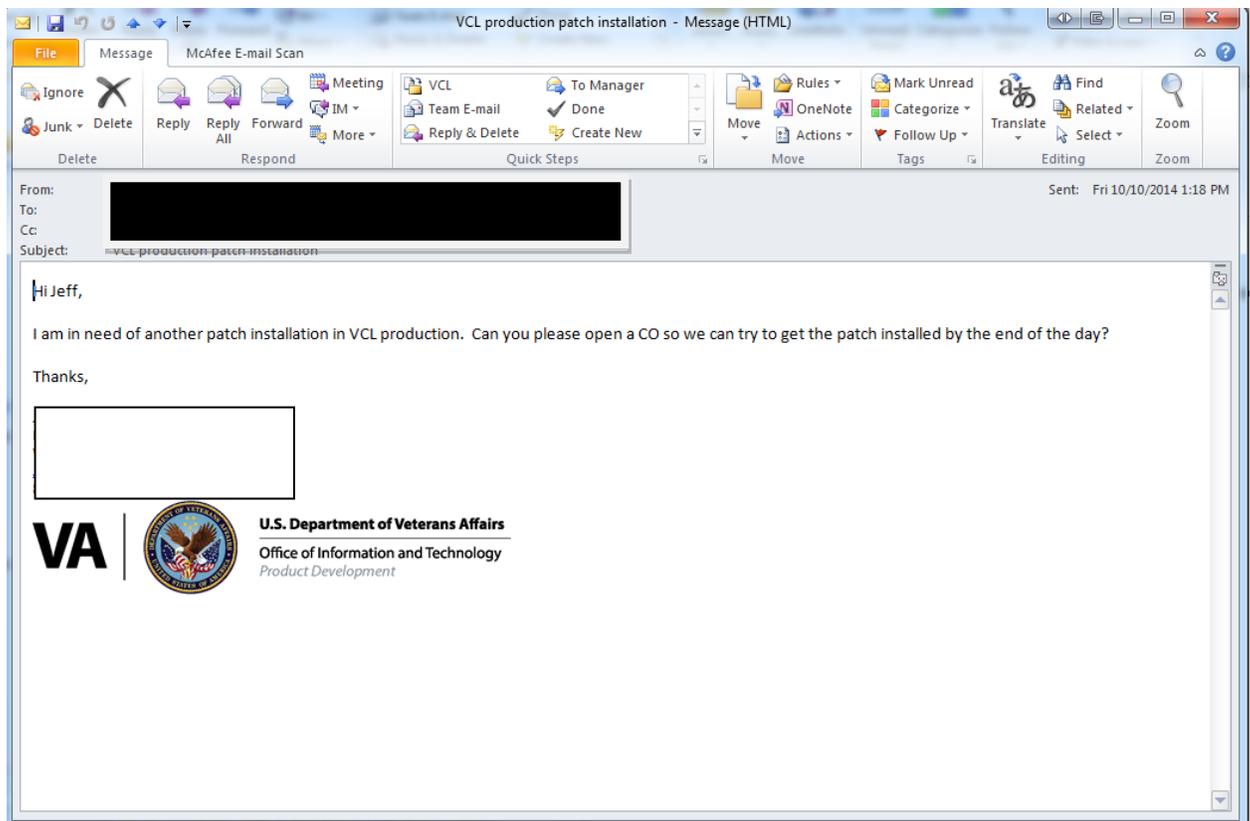


Figure 45: Change Order Request Email

4. Wait for the AITC team to respond back saying they have installed the patch.
5. Verify your patch was installed successfully. If required, have a VCL user log in and verify it for you.

8. Troubleshooting

VCL development team participated with AITC resources during a dry run of the install process and any problems encountered were remediated and incorporated into this guide. VCL developers are available during the installation for assistance.

8.1. Rollback Instructions

For initial release, if there are any issues with the first migration, the rollback plan is to revert back to the Orlando environment.

After initial release, if there are any issues with the VCL application, the necessary action is to roll back to the last clean working version. The database admin and system admin should determine the correct last working version to rollback to.

The following are the steps to return the VCL database to its last working version:

1. Restore database "**NationalSuicideHotline_Test**" from the backup version from step 7 of the above Backout Procedures.

The database restore will clean the database and restore it to the clean state created in step 7 of Section 3.5.3 Backout Procedures.

2. Confirm that the backup and new working application folders are renamed.
3. Test the VCL application and confirm that the restored version is working correctly.

Refer to section 6.6 of the [ISCP](#) for key contacts in the event that a rollback for the VCL software is needed.

9. FAQ

Question	What do I do if I have installation issues?
Response	1. If assistance is needed during installation, please create a Remedy Ticket or contact the REDACTED
Question	How can I check my connection to the broker server?
Response	<ol style="list-style-type: none"> 1. Check the windows registry (HKLM/software/vista/broker/servers) key and ensure that the key is set to the correct IP and port. 2. Check that the broker is running on the correct instance of VistA and on the correct port. <ul style="list-style-type: none"> • Type D ^%SS to show the list • Find the instance and find the line XWBTCPL • Verify that the TCP port number is correct
Question	How can I check the Windows application Event Notifier?
Response	<ol style="list-style-type: none"> 1. Right-click My Computer. 2. Select Manage. 3. Expand Event Viewer. 4. Select Application.
Question	How do I stop the CP Gateway Service?
Response	<ol style="list-style-type: none"> 1. In Windows, click Start Control Panel Administrative Tools Services. The Services window displays. 2. Click the Clinical Procedures Gateway row. A link, Stop the service, displays. 3. Click Stop. A progress window displays as the service stops. 4. When the progress window closes, the Services window redisplay. The status column in the Clinical Procedures Gateway row displays Stopped.
Question	How can I change the time interval for CP Console and CP Flowsheets at which they time out?
Answer	The time interval is set using the TIMED READ value in the NEW PERSON file (#200).
Question	What are the post-deployment requirements for testing the successful install?
Answer	<ul style="list-style-type: none"> • Verify the code deployment

	<ul style="list-style-type: none">• Validate connections with other systems
--	---